



# Cellebrite UFED and Responder

Performing extractions

May 2021 | Version 7.45

## Legal notices

Copyright © 2021 Cellebrite DI Ltd. All rights reserved.

This document is delivered subject to the following conditions and restrictions:

- » This document contains proprietary information belonging to Cellebrite DI Ltd. Such information is supplied solely for the purpose of assisting explicitly and properly authorized users of the Cellebrite UFED/Responder.
- » No part of this content may be used for any other purpose, disclosed to any person or firm, or reproduced by any means, electronic or mechanical, without the express prior written permission of Cellebrite Ltd.
- » The text and graphics are for the purpose of illustration and reference only. The specifications on which they are based are subject to change without notice.
- » Information in this document is subject to change without notice. Corporate and individual names and data used in examples herein are fictitious unless otherwise noted.

<b>1. Overview</b>	<b>7</b>
1.1. System requirements	8
1.2. Extraction types	9
1.3. Accessories	10
1.3.1. Cellebrite UFED Device Adapter with USB 3.0	11
1.3.2. Multi SIM Adapter	13
1.3.3. Using cables and tips	13
1.4. Supported devices	14
1.5. Cellebrite YouTube channel	14
<b>2. Logical extraction</b>	<b>15</b>
2.1. Advanced logical Android extraction	16
2.1.1. The extracted data folder	16
2.2. Advanced logical iOS extraction	17
2.2.1. Encrypted iTunes backup	20
2.3. Logical (Partial)	21
2.4. Logical extraction via Bluetooth	24
<b>3. Password extraction</b>	<b>29</b>
3.1. Extracting the user lock	29
3.1.1. The extracted passwords folder	32
3.2. Disabling or re-enabling the user lock	33
3.3. Removing the screen lock	35
<b>4. File system extraction</b>	<b>38</b>

4.1. Performing a file system extraction .....	38
4.1.1. The file system extraction folder .....	40
4.2. Android backup .....	41
4.2.1. Extracted apps .....	44
4.3. Android backup APK downgrade .....	45
4.3.1. Android backup APK downgrade - Manual installation .....	50
4.4. Vendor backup .....	53
4.4.1. LG backup .....	53
4.5. Selective file system extraction .....	56
<b>5. Physical extraction .....</b>	<b>59</b>
6.1. Performing a physical extraction .....	60
6.1.1. The Physical extraction folder .....	62
6.2. ADB rooted .....	63
6.3. Advanced ADB .....	65
6.3.1. Generic model .....	73
6.3.2. Errors and notifications .....	75
6.4. Boot loader (FW flashing) .....	82
6.5. Decrypting boot loader .....	85
6.6. Forensic recovery partition .....	87
6.7. Smart ADB .....	91
<b>7. Capture images and screenshots .....</b>	<b>95</b>
7.1. The Cellebrite UFED camera .....	95
7.2. Capturing images .....	96



7.3. Capturing screenshots .....	100
<b>8. Chat capture .....</b>	<b>102</b>
8.1. Performing a Chat capture by application .....	102
8.2. Performing a Chat capture in Generic mode .....	104
<b>9. SIM card functionality .....</b>	<b>107</b>
9.1. SIM data extraction .....	107
9.1.1. Performing SIM data extraction .....	107
9.2. Clone SIM .....	111
9.2.1. Cloning an existing SIM card ID .....	111
9.2.2. Entering SIM data manually .....	114
9.2.3. Creating a GSM test SIM .....	118
<b>10. Drone extractions .....</b>	<b>119</b>
<b>11. Device tools .....</b>	<b>122</b>
11.1. Activate TomTom trip log .....	124
11.2. Android Debug Console .....	124
11.3. Bluetooth scan .....	126
11.4. Disable iTunes encryption password .....	126
11.5. Exit Android recovery mode .....	127
11.6. Exit Motorola Bootloop .....	127
11.7. Exit Odin mode .....	127
11.8. Flash Cable 500 Firmware .....	127
11.9. LG EDL recovery .....	128
11.10. Nokia WP8 recovery tool .....	128

11.11. Remove Android extraction files .....	128
11.12. Samsung Exynos Recovery .....	128
11.13. Saved APKs from APK downgrade .....	129
11.14. Switch to CDMA offline mode .....	130
11.15. Uninstall Windows mobile client .....	131
<b>12. Glossary .....</b>	<b>132</b>
<b>13. Index .....</b>	<b>133</b>

# 1. Overview

Cellebrite UFED/Responder is a new generation solution that empowers law enforcement, military, intelligence, personnel to capture critical forensic evidence from Android and iOS mobile devices.

Cellebrite UFED/Responder enables you to:

- » Perform physical, file system, and logical extraction of device data and passwords. Capabilities may vary, based on the Cellebrite UFED/Responder product purchased - Cellebrite UFED/Responder Logical or Cellebrite UFED/Responder Ultimate.
- » Extract vital data such as call logs, phonebook entries, text messages (SMS), pictures, videos, audio files, ESN IMEI, ICCID and IMSI information and more, from a wide range of mobile devices.
- » Extract data from the widest selection of operating systems, such as Apple iOS, Blackberry, Android, Symbian, Microsoft Mobile, and Palm OS.
- » Clone the SIM ID, which allows you to extract phone data while preventing the mobile device from connecting to the network. It can also help if the SIM card is missing.
- » Extract the data from a mobile device either by a cable based connection (serial or USB) or a Bluetooth wireless connection. The tips and cable kit consists of four master cables and various tips.



This manual is also relevant for Cellebrite Responder users.

## 1.1. System requirements

PC	Windows compatible PC with Intel i5 or compatible running at 1.9 GHz or higher	
Operating system	Microsoft Windows 10, 64-bit Microsoft Windows 8.x, 64-bit Microsoft Windows 7, 64-bit Microsoft Windows 7 Boot Camp on MAC	
Memory (RAM)	<b>Recommended</b> 16 GB	<b>Minimum</b> 4 GB
Space requirements	1.5 GB of free disk space for installation	
Additional requirements	Microsoft .Net version 4.5 or later	
Permissions	If you intend to activate the application using a hardware license key (dongle) provided by Cellebrite, you must have administrative rights over the computer.	



This specification is for a PC running both Cellebrite UFED/Responder and the Physical Analyzer application as the decoding operations of Physical Analyzer require the higher specification. For a standalone PC running Cellebrite UFED/Responder an ATOM based chipset (or equivalent) is sufficient.

## 1.2. Extraction types

Cellebrite UFED/Responder includes a range of data extraction types.



The available extractions may vary, based on the type of product purchased; the Cellebrite UFED/Responder Logical or the Cellebrite UFED/Responder Ultimate product.

Table 1-1: Functionalities of the Cellebrite UFED/Responder products

Functionality	Cellebrite UFED/Responder Logical	Cellebrite UFED/Responder Ultimate
Logical Extraction	Yes	Yes
SIM Data Extraction	Yes	Yes
Password Extraction	Yes	Yes
Clone SIM	Yes	Yes
File System Extraction	Not available	Yes
Physical Extraction	Not available	Yes
Capture Images/Screenshots	Optional	Yes
Chat capture	Yes	Yes

The extraction types are:

- » **Logical extraction:** Extracts user data from a mobile device (SMS, call logs, pictures, phonebook, videos, audio, certain application data, and more). Quickest extraction method but least amount of data.
- » **SIM card extraction:** Extracts data from a SIM or USIM card.
- » **File system extraction:** Extracts files embedded in the memory of a mobile device. Retrieve the artifacts within a Logical extraction, in addition to hidden system files, databases and other files which were not visible within a logical extraction.
- » **Password extractions:** Unlocks and displays passwords from a source mobile device.
- » **Clone SIM:** Copies a SIM ID from one SIM card to another SIM card or to a Cellebrite UFED SIM ID Access Card.
- » **Physical extraction:** Extracts a physical bit-for-bit image of the flash memory of a device, including the unallocated space using advanced methods. Unallocated space is the area

of the flash memory that is no longer tracked by the file system, which may contain images, videos, files, and more.

- » **Capture images and screenshots:** Take pictures or videos of a device using the Cellebrite UFED camera. You can also capture internal screenshots directly from the connected device.
- » **Chat capture:** Chat Capture is an automated screen capturing process that allows users to extract and analyze selective chat conversations from third party application data.

### 1.3. Accessories

The Cellebrite UFED kit includes connection cables and tips. These are used in order to connect mobile devices to Cellebrite UFED.



Figure: Cellebrite UFED Cables and tips

The Cellebrite UFED Ultimate kit contains tips and cables for logical, file system, and physical extractions.

The Cellebrite UFED Logical kit contains tips and cables for Logical Extraction only.

### 1.3.1. Cellebrite UFED Device Adapter with USB 3.0

The Cellebrite UFED kit contains a device adapter that attaches to your PC's USB ports. Each connector has a LED that indicates availability during an extraction and blinks to indicate where to connect the source device. In addition, there are LEDs for power and Bluetooth.

Depending on when you received your kit, there are two types of device adapters: Cellebrite UFED Device Adapter with USB 3.0 (latest version) and Cellebrite UFED Device Adapter with USB 2.0 (previous version). This document provides more information on the Cellebrite UFED Device Adapter with USB 3.0.



This manual is also relevant for Cellebrite Responder users.



Some devices can be extracted only by using the Cellebrite UFED Device Adapter.



This device adapter has the following connectors:

- » GPIO port (for future use)
- » USB 3.0 port
- » RJ45 port
- » DC In power supply (Input 5.3V 3.7A)
- » 2 USB connection cables labeled POWER and DATA.

For information on the specifications, refer to the *Overview Guide*.

### To connect the Cellebrite UFED Device Adapter with USB 3.0:

1. First connect the DATA cable to a USB port on the computer.
2. Then connect the POWER cable to a second USB port on the computer.



Use the following procedure, if the computer is mounted in a difficult to access or distant location.

### To connect the Cellebrite UFED Device Adapter with USB 3.0 using extension cables:

1. Connect the Active Extension cable to the DATA connection cable. Refer to the *Overview Guide*.
2. Connect the other end of this extension cable to a USB port on the PC.
3. Connect a standard USB extension cable to the POWER connection cable.
4. Connect the other end of this extension cable to a USB port on the PC.





#### 1.3.1.0.1. Using the External power supply

The external power supply is NOT required for the smooth operation of the Cellebrite UFED Device Adapter V3, but is provided for those cases where additional power output is required. The external power supply provides an output of approximately 5.3V 2.7A.

#### 1.3.2. Multi SIM Adapter

A Multi SIM Adapter supports Micro, Nano and standard SIM cards.



It is recommended to connect the Multi SIM Adapter to an available USB port on your computer, not to the USB port on the Cellebrite UFED Device Adapter.



#### 1.3.3. Using cables and tips

The cables and tips include various adapter cables (the number of cables depends on the Cellebrite UFED product and kit purchased). Each cable has a letter and name for example: A Adapter – USB.



*Figure: Single cable*

For easy recognition, the tips are color coded and numbered; the color represents the vendor.



*Figure: Cellebrite UFED tip (example)*

Before each extraction, the required cable and tip number and color is specified in the **Source** area of the Select Content Types screen.

## 1.4. Supported devices

To find out which mobile devices are supported in Cellebrite UFED and which data extraction capabilities are available for every mobile device use one of the following:

1. The Cellebrite UFED <version no> Supported Phone List file is delivered with every Cellebrite UFED software version update. The Microsoft Excel file contains two worksheets:

The **Cellebrite UFED Logical** sheet lists the mobile devices supported for logical extraction.

The **Cellebrite UFED Physical** sheet lists the mobile devices supported for physical, file system, and password extractions.

2. **UFED Phone Detective** (devices supported for logical extraction only).
3. Cellebrite UFED Supported Devices document in [MyCellebrite](#).

## 1.5. Cellebrite YouTube channel

For your convenience, a selection of useful videos demonstrating typical workflows and common procedures are available at [youtube.com/cellebriteufed](https://youtube.com/cellebriteufed).

## 2. Logical extraction

The Logical Extraction function enables you to extract various types of data, such as call logs, phonebook records, SMS text messages, calendar events, and multimedia files (images, videos, etc.). Save the extracted data from the source device to your PC or to a removable storage device, as desired. In most cases, a logical extraction is not possible for locked devices.

A logical extraction can also be used to extract data from many Android, BlackBerry, iOS, and Windows Phone apps. For an updated list of supported apps and versions for each platform go to **Help > Supported Apps** in Physical/Logical Analyzer. Data extracted from these apps can be analyzed using Physical/Logical Analyzer (although the data is not included in UFED HTML and XML reports).



The available types of extracted data may vary depending on the source device manufacturer and model. The supported data types are listed in the UFED Phone Detective or within the [UFED Supported Devices](#).

Logical extraction includes the following:

[Advanced logical Android extraction \(on the next page\)](#)

[Advanced logical iOS extraction \(on page 17\)](#)

[Logical \(Partial\) \(on page 21\)](#)

[Logical extraction via Bluetooth \(on page 24\)](#)

## 2.1. Advanced logical Android extraction

The following procedure explains the Advanced logical extraction process for an example device. The procedure may vary depending on the selected device. This section shows only one of the many extraction types that can be performed.

### 2.1.1. The extracted data folder

At the end of the data extraction process, the extracted data is saved in the location you selected.



The extracted data folder is named "UFED" with the selected device name, the IMEI/MEID info. and the extraction date. For example, "UFED Samsung GSM GT-i9205 Samsung Galaxy Mega 6.3 2014\_11\_10 (0001)"

The extracted data folder contains:

- » Multimedia files folders named Audio, Images, Ringtones, and Video folders, containing each of the respective type of media files.
- » Phone extraction report files in HTML and XML formats. (One HTML report per content type)
- » Cellebrite UFED Manager files of the extracted calls log (\*.clog), phonebook (\*.pbb), SMS messages (\*.sms), and calendar (\*.cal) Email(\*.Email), MMS(\*.MMS) and IM(\*.IM) data.
- » UFD file.



UFED Manager files are generated only for data types that contain items.

The XML file can be viewed by both Logical Analyzer and Physical Analyzer.

## 2.2. Advanced logical iOS extraction

The Advanced logical extraction uses other extraction protocols and can potentially extract additional data compared to the standard logical extraction.

Advanced logical extractions can be used to extract data from Android or iOS operating systems. The following example shows an Advanced logical iOS extraction.

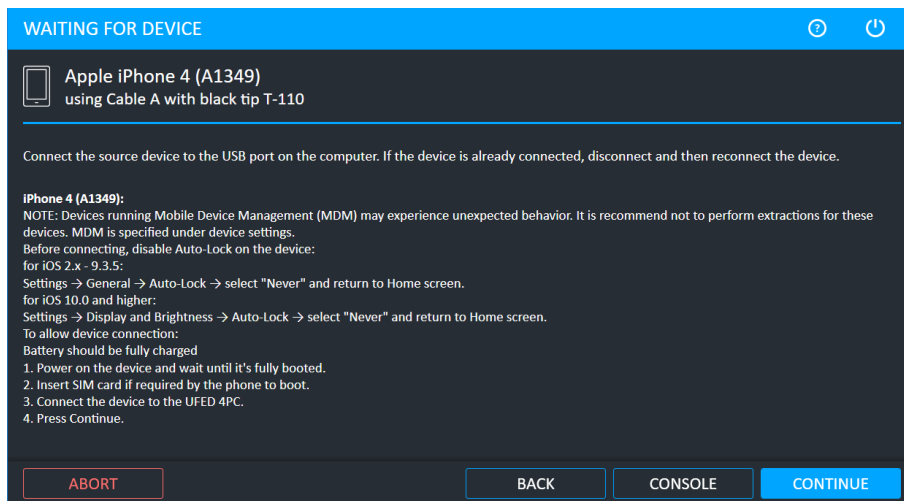
### To perform an advanced logical iOS extraction:

1. Click **Mobile device** and identify the device.
2. Click **Advanced Logical**.



For information on using optional timeframe and party filters, refer to the *Overview Guide*.

The following window appears.



3. Connect the source device to the USB port using the specified cable. If the device is already connected, disconnect and then reconnect the device.
4. Click **Continue**. The following window appears.

### Source Instructions

Please unlock the device and choose 'Trust' when the trust message displays.

**Note:** Devices with iOS 11 may also require the device password. If the password is requested enter it to proceed with the extraction.

5. Unlock the device and select **Trust** on the device. The following window appears.

### Attention

Device: jonathank's iPhone

UDID: d6941ce78b1ba2276ad4ebd93d5019c74ed71158

iOS: 7.0.4

Backup: Not encrypted

OK

6. This window displays the device name, UDID, iOS version, and whether the backup is encrypted. Click OK. If the iTunes backup is not encrypted, the following message about data encryption appears. If the iTunes backup is encrypted, see [Encrypted iTunes backup \(on page 20\)](#).

### Attention

To extract user credentials from an iOS device, backup encryption should be enabled (encryption is automatically disabled at the end of a successful extraction).

Enable backup encryption? (UFED will temporary set the password to "1234".)

NO

YES

7. In the Attention window click **Yes** to enable backup encryption with the ability to extract additional information from the device, or click **No** if you do not require the additional information. The following window appears.



There is an option to encrypt the iOS file. This additional layer of security allows iOS to include more sensitive information not found on a standard iCloud or iTunes backup file, including login details for apps and email accounts and other services that may be in use. You can extract an iOS keychain (user credentials) using this extraction method. At the end of the extraction, the encryption will automatically be reset. You can view the user credentials under the Passwords tree item in Physical Analyzer.



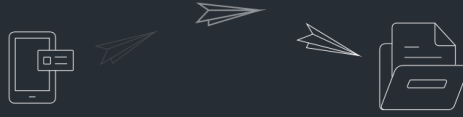
If the extraction was stopped and the device remains encrypted, see [Disable iTunes encryption password \(on page 126\)](#).

EXTRACTION IN PROGRESS



Apple iPhone 4 (A1349)  
using Cable A with black tip T-110

Please wait, this can take some time...



/Facebook.app/Facebook

ABORT

### 2.2.1. Encrypted iTunes backup

During Advanced Logical Extraction, if iTunes backup encryption is already enabled, then the following window appears:

**Source**  
**Encrypted Backup Password**  
iTunes backup encryption is enabled.  
To preserve the password for the decoding stage enter it below (or press "Skip" if not known).  
Note: If you cannot obtain the password (including brute-force attempts), contact Cellebrite CAIS to bypass the iTunes encryption.  
  
☐ Show Characters

#### If you know the iTunes backup password:

1. Enter the password so that it will not be required during the decoding stage (in Physical Analyzer).
2. Click OK and follow the on-screen instructions to complete the extraction.

#### If you do not know the iTunes backup password:

- » Click **Skip** and follow the on-screen instructions to complete the extraction.



The password will be required during the decoding stage (in Physical Analyzer).



If you have exhausted all options to obtain the password (including the brute-force option), Cellebrite Services can provide a full file system extraction that will bypass the iTunes encryption.



## 2.3. Logical (Partial)

This is a quick extraction method that supports the largest number of devices. You can extract Call logs, Phone books, SMSs, Calendar events, Multimedia files, and file data. The available types of data may vary depending on the source device's make and model. In most cases, a logical extraction is not possible for locked devices.

### To perform Logical (Partial) extraction:

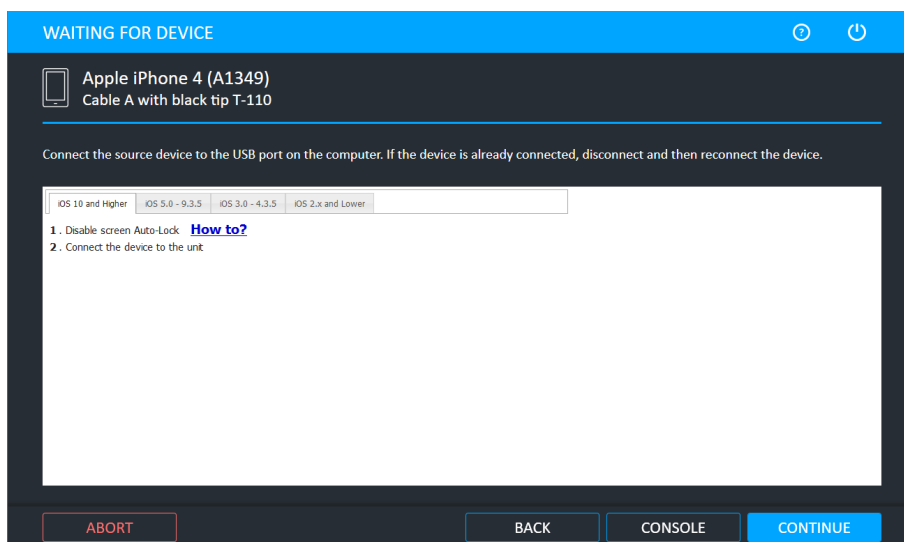
1. Click **Mobile device** and identify the device.
2. Click **Logical (Partial)** and then select where you want to save the extraction.



For information on using optional timeframe and party filters, refer to the *Overview Guide*.

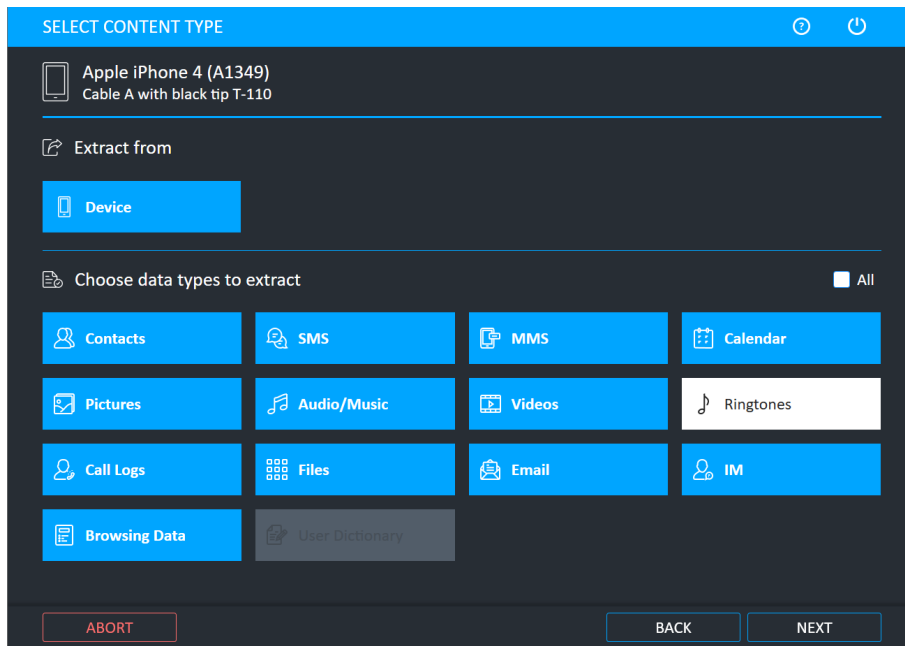
The Select Extraction Location window appears.

3. Use the current location or click the folder icon to change the target path and select a different location and then click **Next**. The Waiting for Device window appears.



The Console button is only supported on Android devices.

4. Select the correct cable and tip for the mobile device, and change the device settings according to the instructions.
5. Connect the source device to a USB port. If the device is already connected, disconnect and then reconnect the device.
6. Click **Continue**. The following window appears.



7. Different data types can be extracted. Select which data types you want to extract. In the example above Ringtones are excluded and will not be extracted.



When the **Files** button is selected, UFED performs an iTunes backup to extract user data.

8. Click **Next**. The following window appears.



### Source Instructions

Please unlock the device and choose 'Trust' when the trust message displays.

**Note:** Devices with iOS 11 may also require the device password. If the password is requested enter it to proceed with the extraction.

9. Unlock the device and select **Trust** on the source device.

Please select multimedia types to extract

Multimedia types	Files	Size	Estimated time
<input checked="" type="checkbox"/>  Pictures	38	24.2 MB	00:00:10
<input checked="" type="checkbox"/>  Videos	3	7.2 MB	00:00:01

Estimated extraction time:

00:00:11

Estimated size:

31.4 MB

OK

Abort

10. Select the multimedia types required and then click OK.

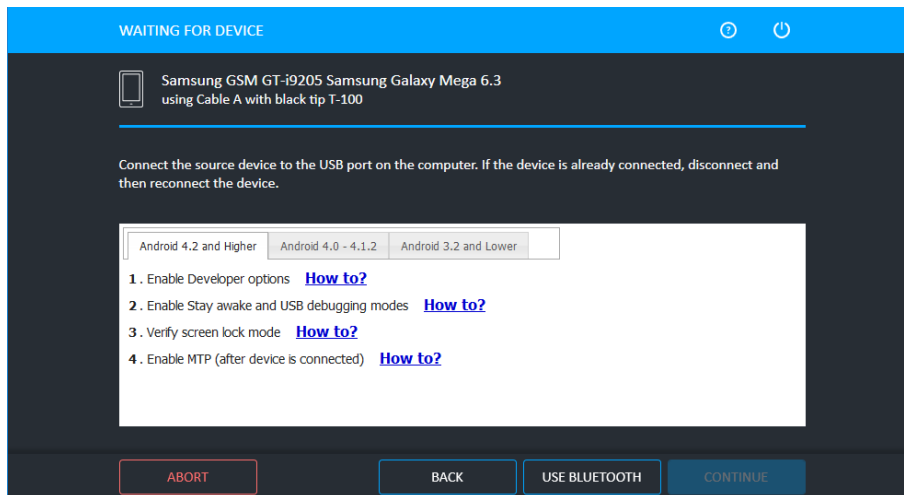
## 2.4. Logical extraction via Bluetooth

This extraction option can be used to perform logical extraction via Bluetooth from any Android device. To use this extraction method, you need to load a client onto the source device over the Bluetooth connection. When extracting data from a device via a Bluetooth connection, some content types (e.g., apps data, pictures, audio/music, video, and ringtones) and memory types (e.g., memory card or SIM card) are not supported. To extract multimedia content via Bluetooth, go to **Smart Phones/PDAs > Android Bluetooth > Logical Extraction > Logical (Only Multimedia)**. Note that this option takes much longer.

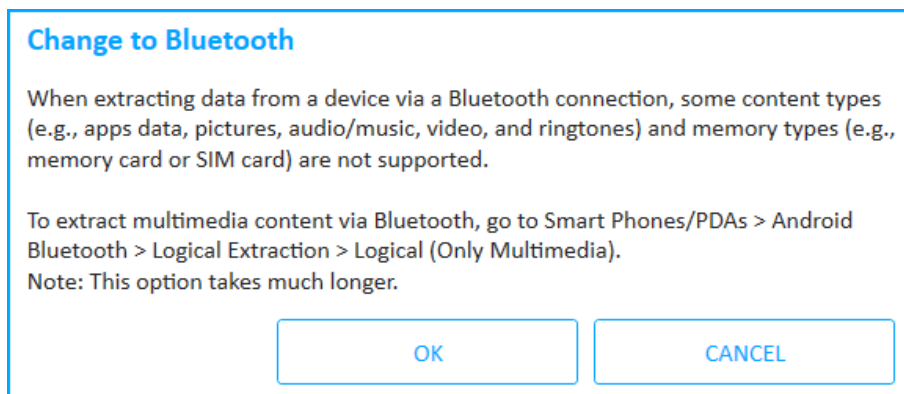
Previously, the logical extraction via Bluetooth option was only available via the generic profile.

### To perform a logical extraction via Bluetooth:

1. Click **Mobile device**, identify the device and then click **Logical**.
2. Select the extraction location. The following window appears.

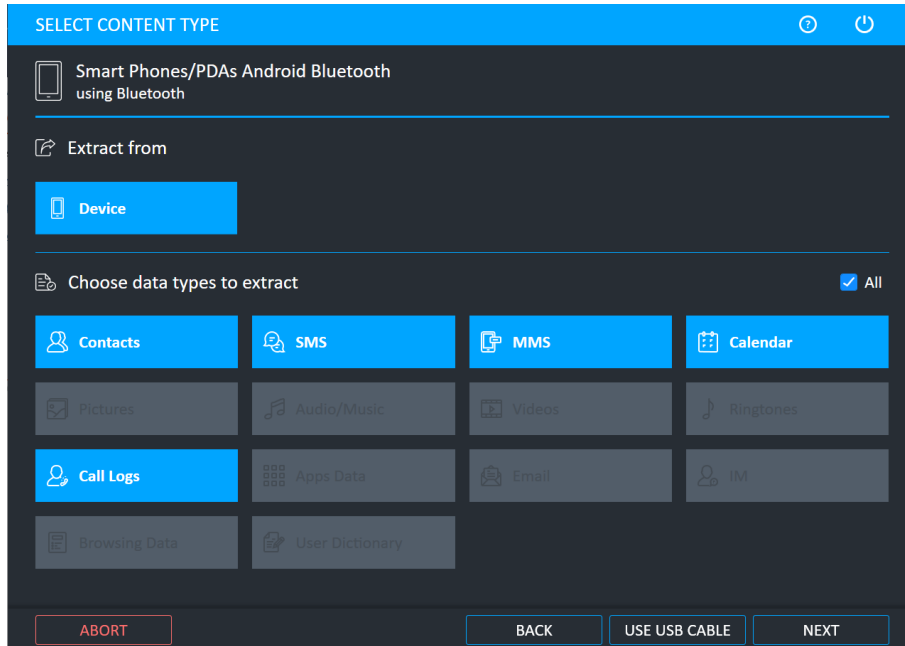


3. Click **Use Bluetooth**. The following window appears.

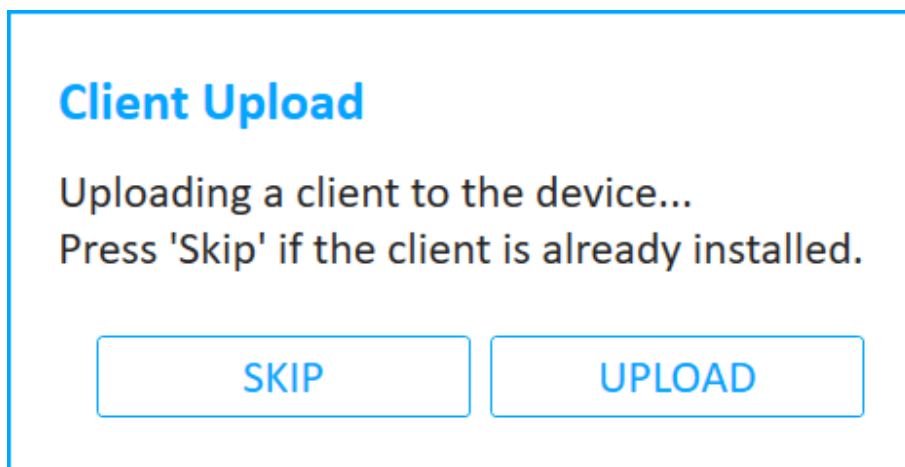


4. Click OK.

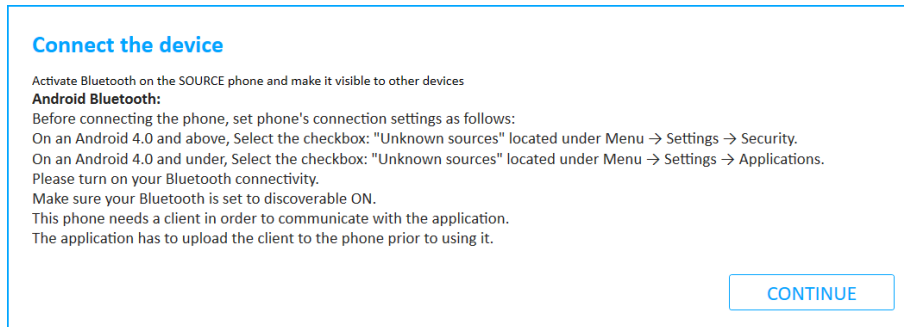
The following window appears.



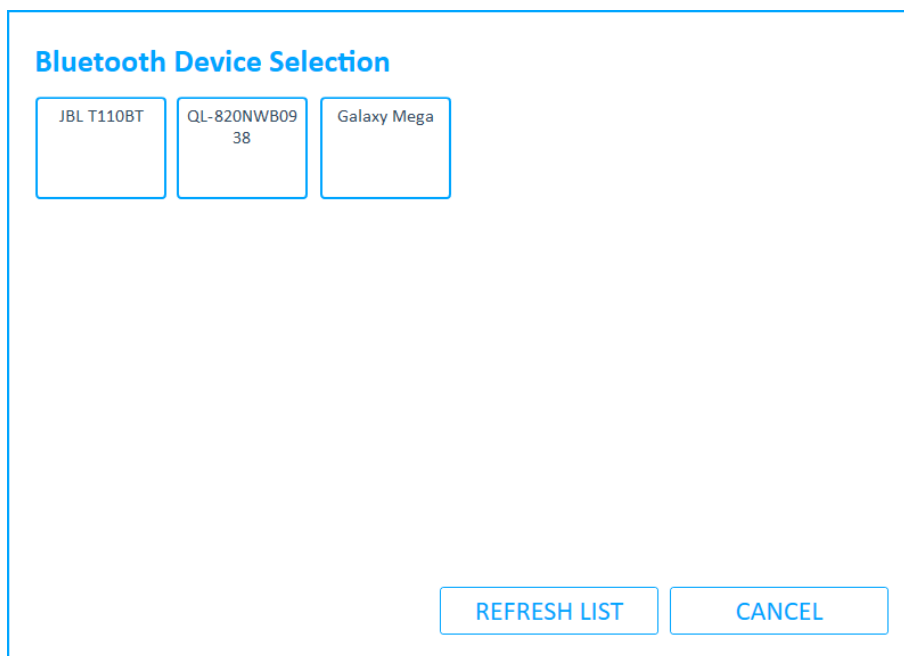
5. Select the required content types and then click **Next**.



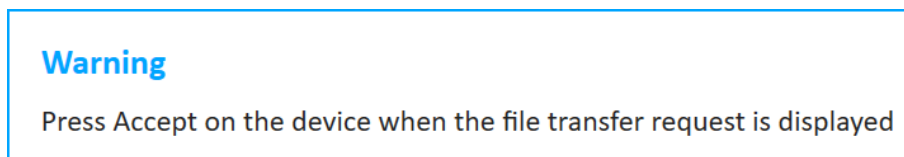
- Click **Upload** to upload the client to the device or click **Skip** if you have already uploaded the client to the device. The following window appears.



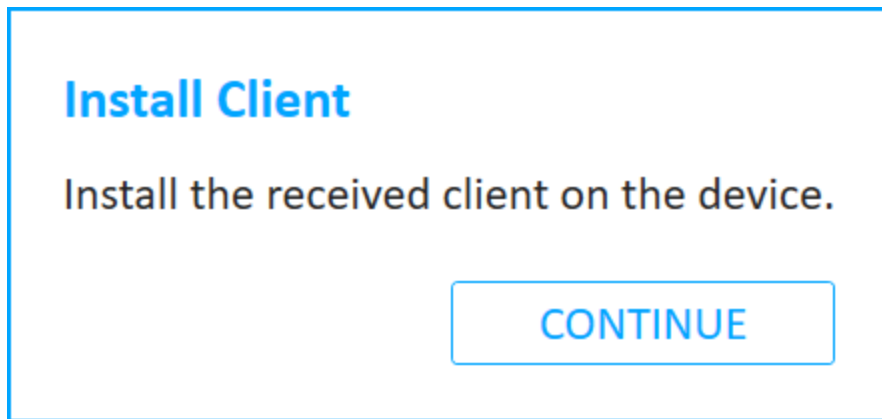
- Activate Bluetooth on the source device and make it visible to other devices. Follow the on-screen instructions to set the devices connections, then click **Continue**. The following window appears.



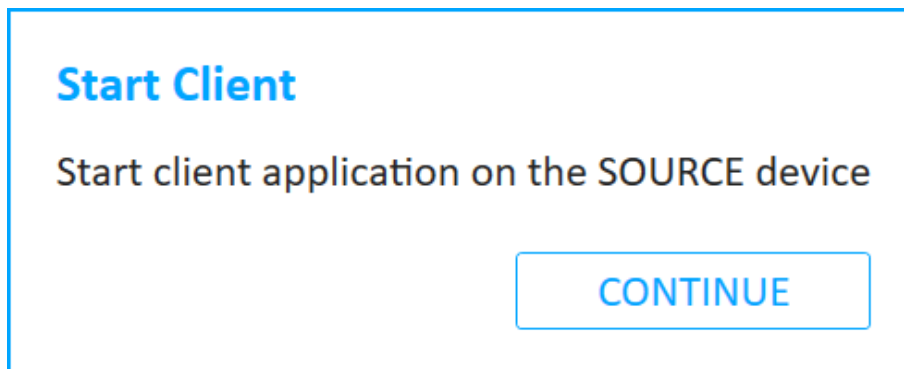
- Click the required device. The following window appears.



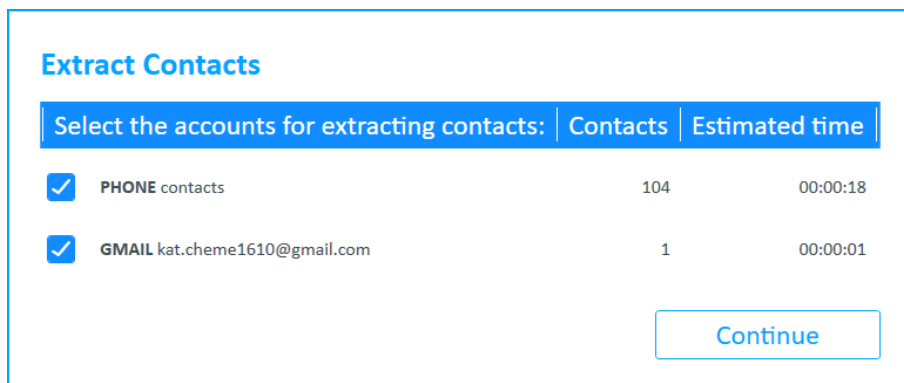
- Press **Accept** on the device when the file transfer request is displayed (this is skipped if the client is already installed). The following window appears.



10. Follow the instructions to install the client on the source device, then click **Continue**.



11. Open (or start) the client on the source device and confirm the Bluetooth permission request on the device.
12. Click **Continue**. The following window appears.



13. Click **Continue**.

During the extraction process, the progress bar for the Source and then the Target is active.

When the extraction is complete and if required, the Source Instructions screen appears (this depends on the device model).

### Source Instructions

**Android Bluetooth:**

Please don't forget to remove the client!

also:

Please restore the connection settings:

On an Android 4.0 and above, Uncheck the checkbox: "Unknown sources" located under Menu → Settings → Security.

On an Android 4.0 and under, Uncheck the checkbox: "Unknown sources" located under Menu → Settings → Applications.

CONTINUE



## 3. Password extraction

It is common to encounter a device that is password protected. Passcodes include a 4-digit PIN, a complex alpha/numeric passcode, or a pattern lock. UFED can identify and bypass some passcodes depending on the make and model of the device. To find out if the passcode can be identified or bypassed, refer to the [UFED Supported Devices](#) file.

Password extraction includes the following:

[Extracting the user lock \(below\)](#)

[Disabling or re-enabling the user lock \(on page 33\)](#)

[Removing the screen lock \(on page 35\)](#)

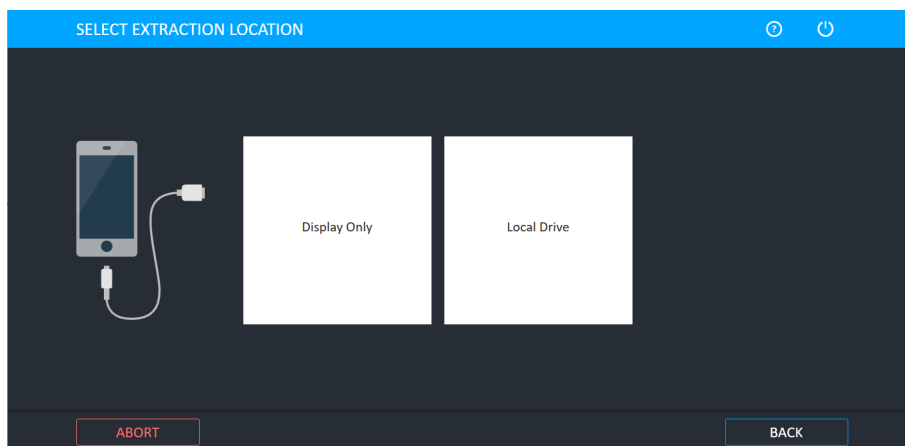
### 3.1. Extracting the user lock

Extract the password, or user code/pin, locking the device. The extracted password can be displayed on the screen or written to a USB flash drive or PC for archiving. The ability to extract passwords depends on the device's make and model, the type of passwords enabled on the device, and the password's length.

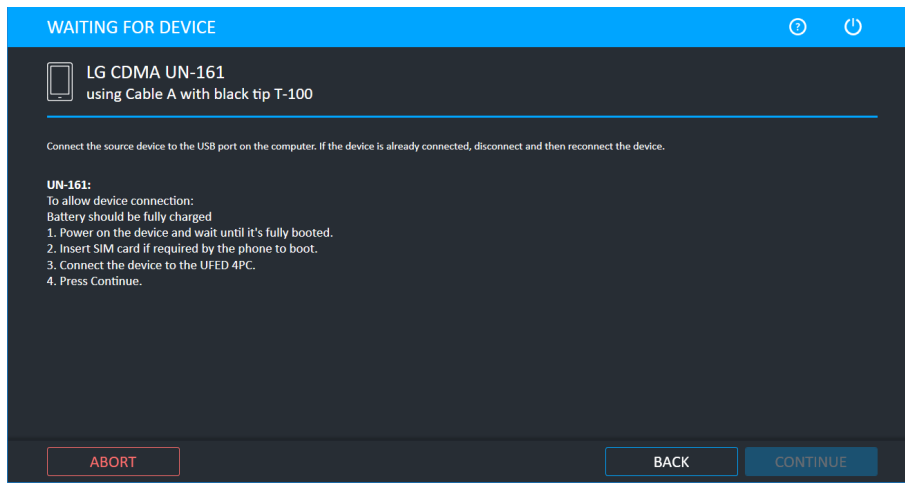
**To extract a user lock on a mobile device:**

1. Click **Mobile device** and identify the device, then click **Extract User Lock**.

The Select Extraction Location screen appears.

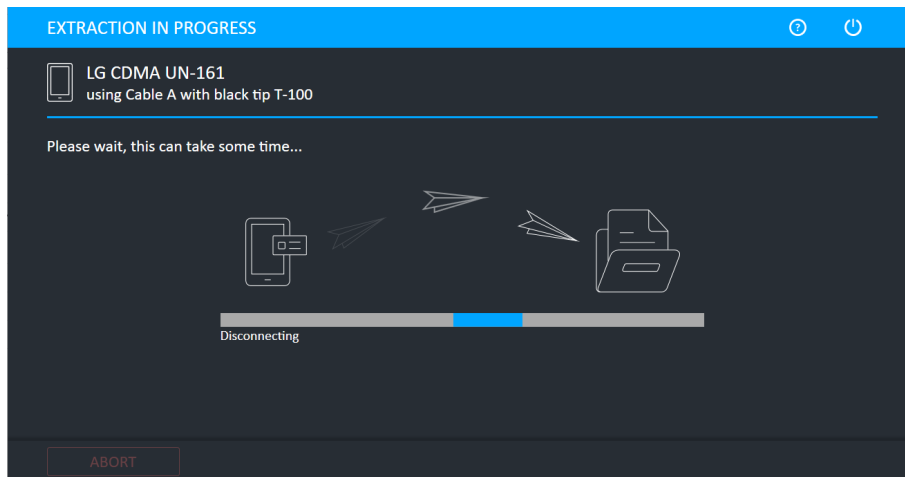


The Waiting for Device screen appears.



2. Connect the source device to the USB port.
3. Click **Continue**.

The Extraction in Progress screen appears.



At the end of the extraction process, the extracted passwords are displayed in the **Passwords** screen.

## Passwords

User Code:

0000

ESN/MEID:

268435459304781538

Own Number:

MIN:

0123450000

CONTINUE

4. Click **Continue** to display a summary of the passwords extraction process.

The following screen appears.

5. Click **Additional Extractions** to add additional extraction types for the same device, or click **Finish** to end the process and return to the Home screen.

### 3.1.1. The extracted passwords folder

At the end of the passwords extraction process, the extracted passwords are saved to a text file named Passwords.txt at the location you selected during the data extraction process.



The text file is located inside a folder named "Password" with the name of the selected device name and the extraction date. For example, "Passwords Iden i9 2011\_06\_11 (001)"

## 3.2. Disabling or re-enabling the user lock

You can disable and re-enable the user lock on a device, as follows:

- » **Disable the user lock:** Disable the user lock (or password), which means that the device will no longer be locked. Each device model has a slightly different process, depending on the device lock combination and how the model connects to UFED. When more than one method is available for the device, it is recommended to try both methods if one method is not successful. If you disable the user lock more than once, you cannot re-enable the original user lock. For a complete list of supported devices, refer to UFED Phone Detective or the UFED Supported Devices document in [MyCellebrite](#).
- » **Re-enable the user lock:** Re-enable the user lock on a device, after it was disabled by UFED. This enables you to return a device to its original state.



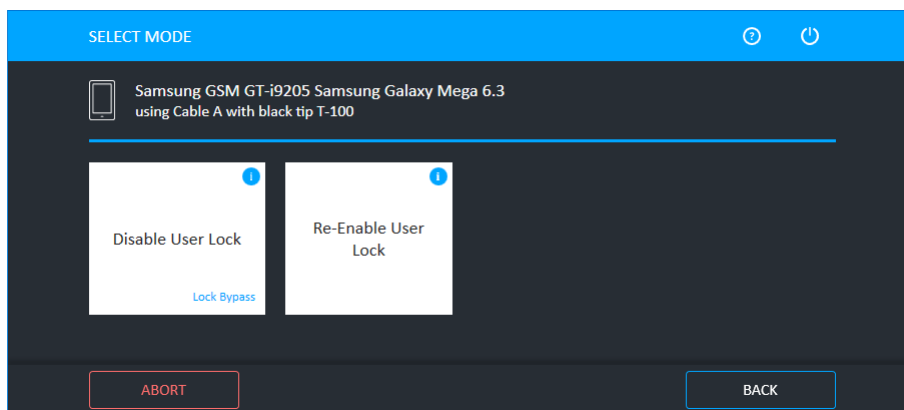
To re-enable the original user lock on the device, use the Re-Enable User Lock method and do not create a new user lock manually. If you create a new user lock, you cannot re-enable the original user lock.



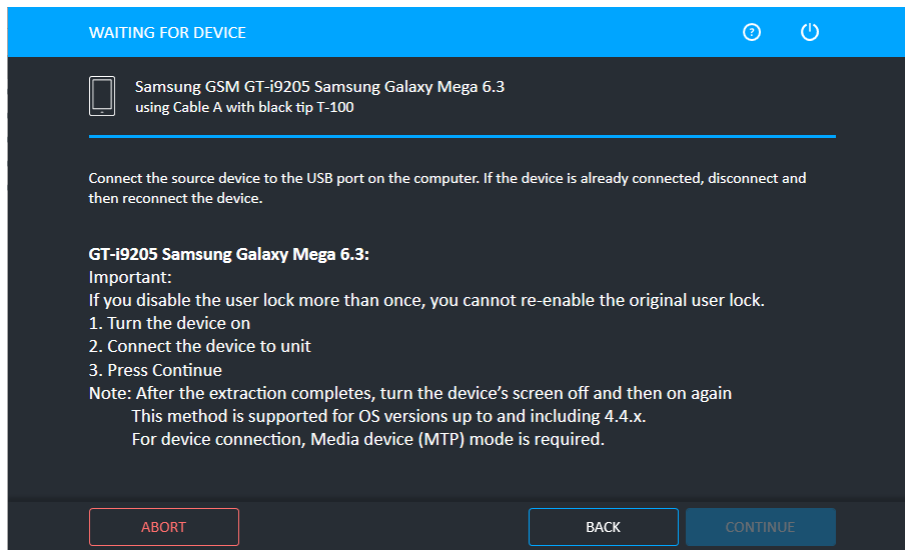
UFED now provides a notification if advanced forensic capabilities are available via Cellebrite Advanced Services for a growing range of supported Android and iOS devices. To learn more refer to: <https://www.cellebrite.com/en/services/advanced-unlocking-services/>

### To disable (or re-enable) the user lock on the device:

1. Click **Mobile device** and identify the device, then click **Disable/Re-enable User Lock**. The following window appears.



2. Click **Disable User Lock** to remove the user lock from the device, or click **Re-Enable User Lock** to re-enable the user lock on the device. The Waiting for Device screen appears.



3. Follow the instructions for the device and then click **Continue**.



If the device does not unlock, click **Abort**, and repeat the procedure. Make sure you are using the correct USB cable.

The Extraction completed successfully screen appears.

4. Click **Finish**.

### 3.3. Removing the screen lock

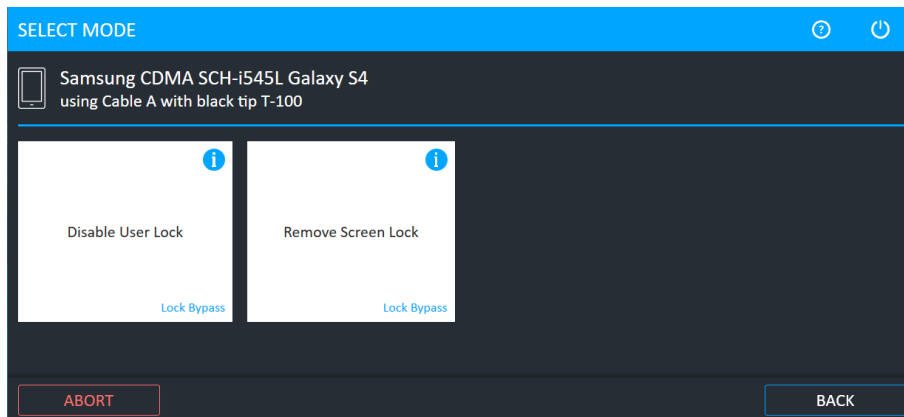
The Remove screen lock method disables the user lock from a wide range of Samsung Android devices for example Galaxy S7, S7 Edge, J7, J5, A7, and A5. This method works on both Qualcomm and Exynos-based devices.



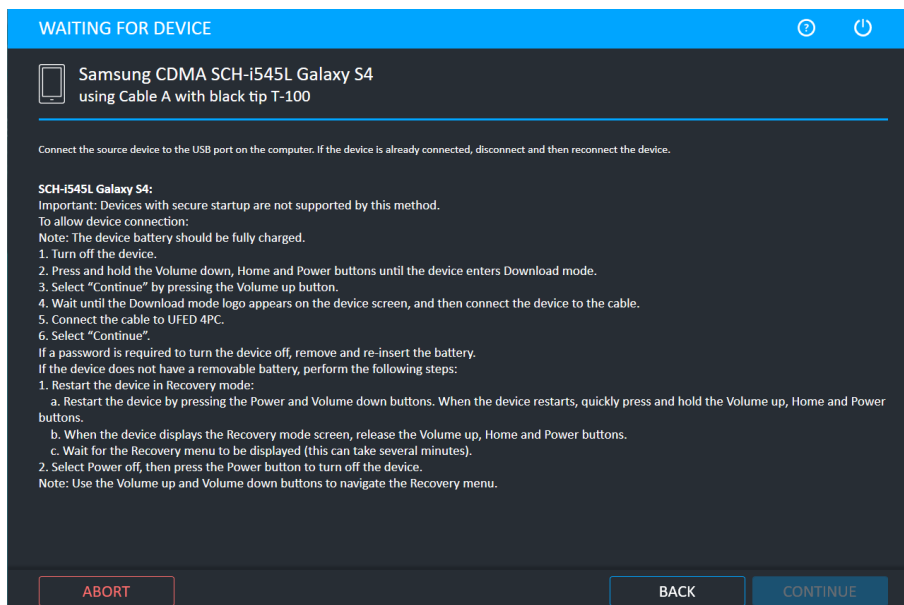
UFED cannot re-enable the screen lock after running the process.

#### To remove the screen lock from a device:

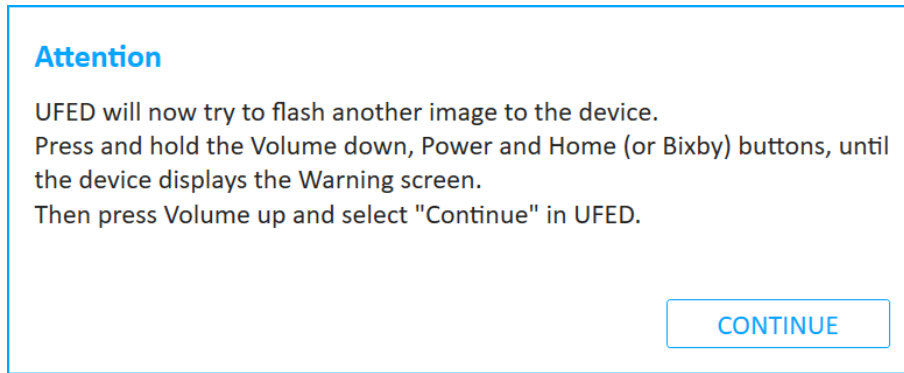
1. Click **Mobile device** and identify the device, then click **Disable/Re-enable User Lock**. The following window appears.



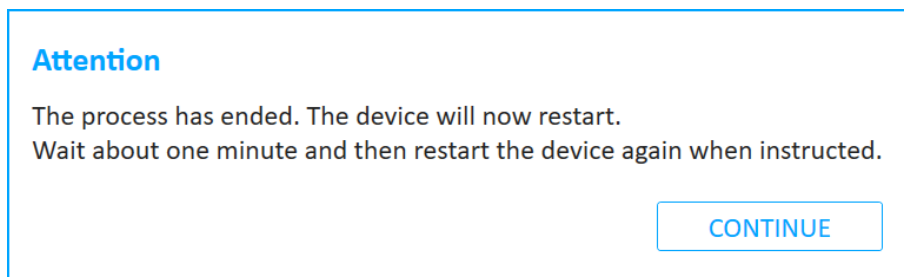
2. Click **Remove Screen Lock** to remove the screen lock from the device. The Waiting for Device window appears.



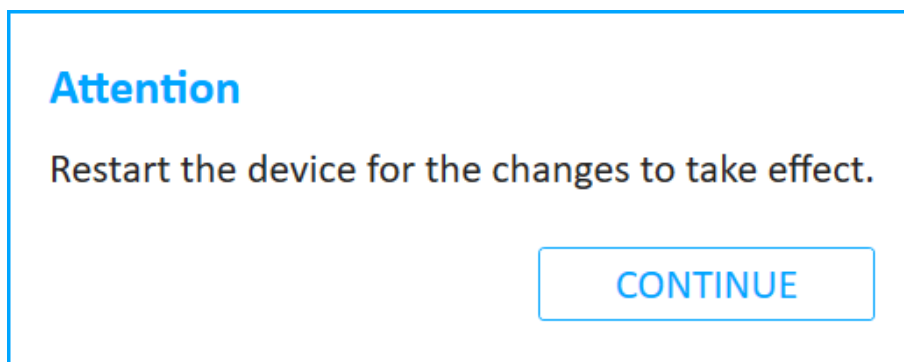
3. Follow the instructions to place the device in Download mode, then click **Continue**. The following window appears.



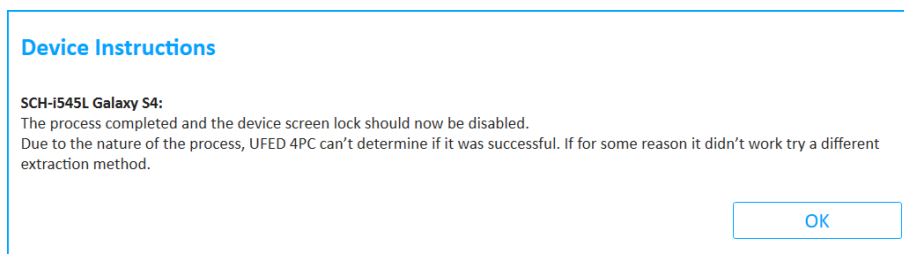
4. UFED will now try to flash another image to the device. Follow the on-screen instructions until the device displays the Warning screen and Download mode again. Then click **Continue** in UFED. The following window appears.



5. Click **Continue**, then wait about one minute and restart the device again when instructed. The following window appears.



6. Restart the device for the changes to take effect and then click **Continue**. The following window appears.

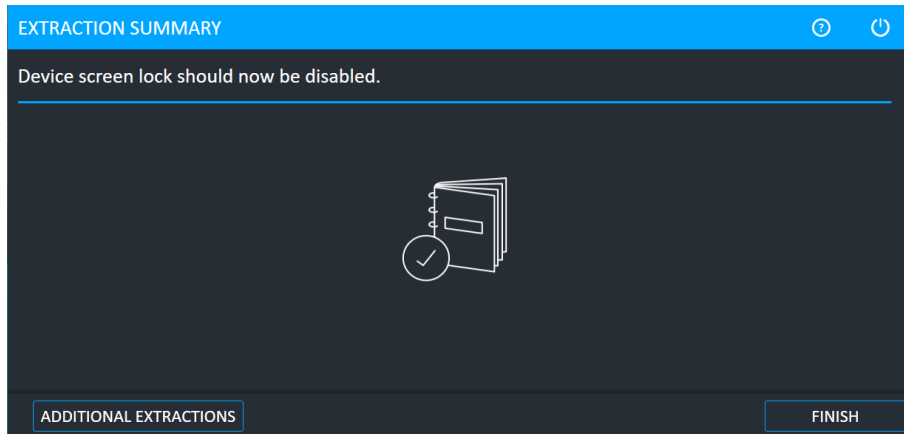






The process completed successfully, but it may not work on all devices.  
If the process did not work, try a different method.

7. Click OK. The following window appears.



8. Click **Finish**.

## 4. File system extraction

The File system extraction enables you to perform a full system extraction from a device.

File system extractions include the following:

[Performing a file system extraction \(below\)](#)

[Android backup \(on page 41\)](#)

[Android backup APK downgrade \(on page 45\)](#)

[Selective file system extraction \(on page 56\)](#)

UFED now provides a notification if advanced forensic capabilities are available via Cellebrite Advanced Services for a growing range of supported Android and iOS devices. To learn more refer to: <https://www.cellebrite.com/en/services/advanced-unlocking-services/>

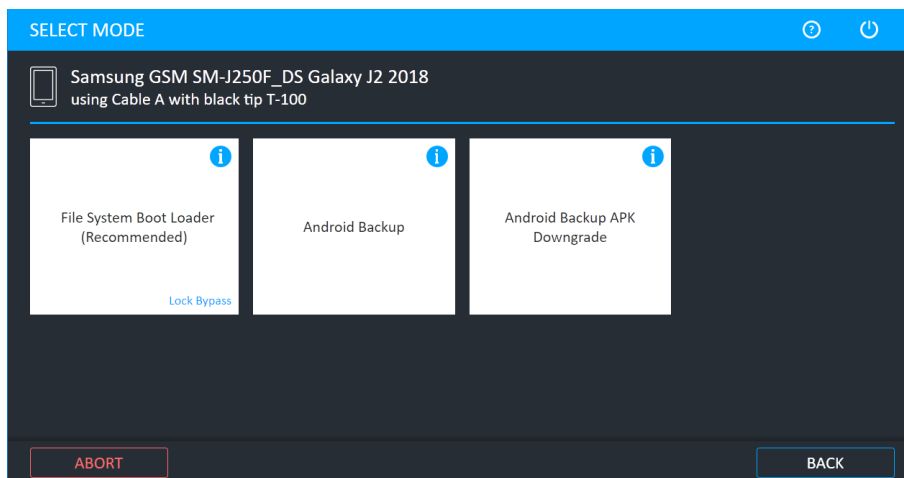


Lock Bypass is displayed if the file system extraction method can bypass the user lock of the device.

### 4.1. Performing a file system extraction

1. Click **Mobile device** and identify the device, then click **File System**.

The Select Mode screen appears.



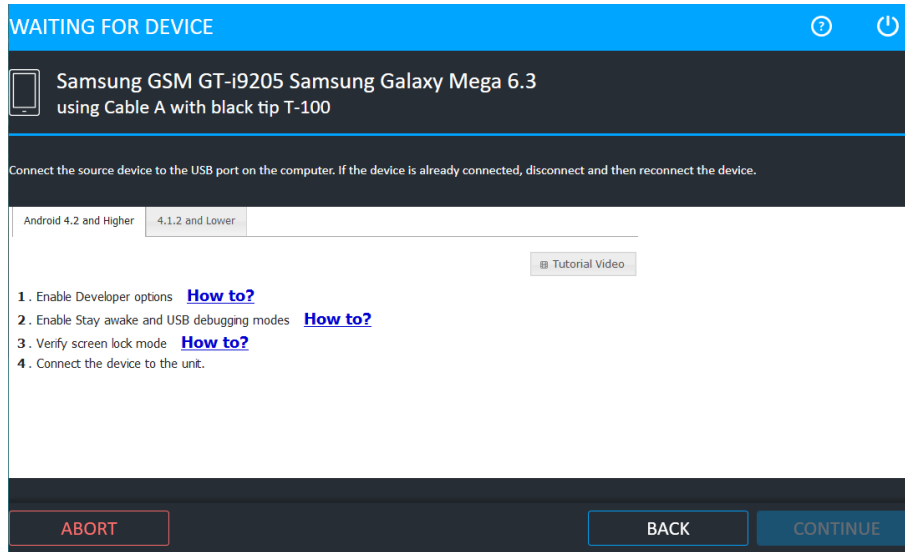
2. Select **ADB** (for Android Backup, see [Android backup \(on page 41\)](#)).



For information on using optional timeframe and party filters, refer to the *Overview Guide*.

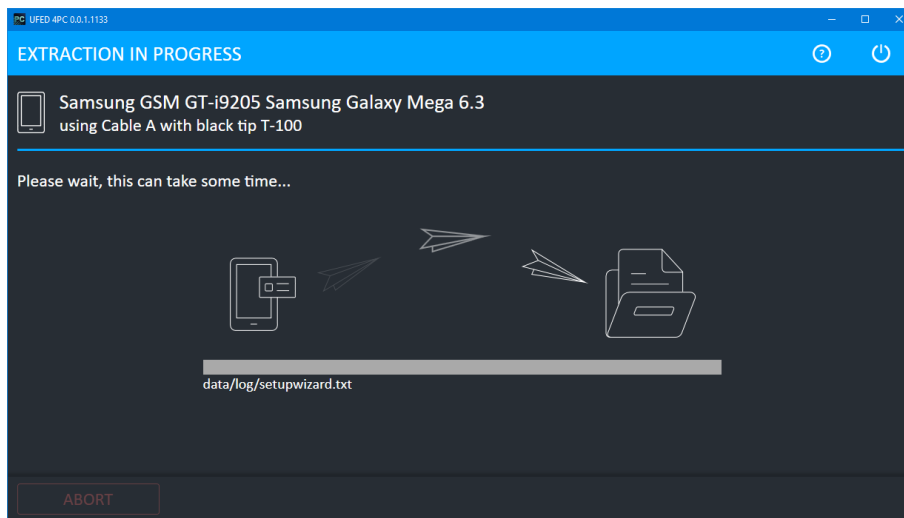
The Select Extraction Location screen appears.

3. Select a location. The following window appears.



4. Select the correct cable and tip for the mobile device based on the information written in the screen.
5. Change the device settings according to the instructions

6. Click **Continue**. The Extraction in Progress screen appears.



During the extraction process, the progress bar for the Source and then the Target is active.



For QCP and Samsung MTK devices, an estimation of the time the extraction will take is displayed.

When extraction is complete, the File System Extraction Summary screen appears.

#### 4.1.1. The file system extraction folder

At the end of the file system extraction process, the extracted data is saved in the location you selected previously (see [Performing a file system extraction \(on page 38\)](#)).



The extracted data folder is named "FileSystemDump" with the selected device model and name and the extraction operation date. For example, "FileSystemDump Nokia GSM Nokia 2626 2014\_03\_12 (001)"

The extracted data folder contains:

- » Zipped archive of the device file system containing files and folders in the same structure they were extracted.
- » UFD file containing the system extraction information, used by the Physical Analyzer application.
- » PM file.

The File System extraction can be viewed using Physical Analyzer.

## 4.2. Android backup

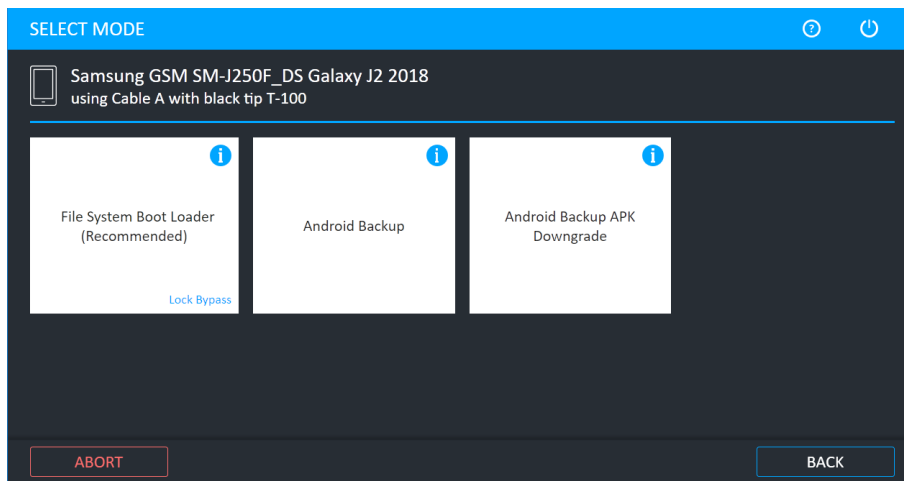
The Android Backup feature communicates with a connected Android device and enables you to extract data from the device. The data that is extracted is dependent on the device's specific characteristics. Android backup supports Android devices with version 4.1 and later.

Android Backup may provide less data than other methods, therefore, you should use this feature when other file system methods such as ADB are not successful, or when other file system methods are not available for the device (for example, if the Android version is not supported).

This feature is controlled under **Settings > General**.

### To extract data using Android backup:

1. Click **Mobile device** and identify the device, then click **File System**.



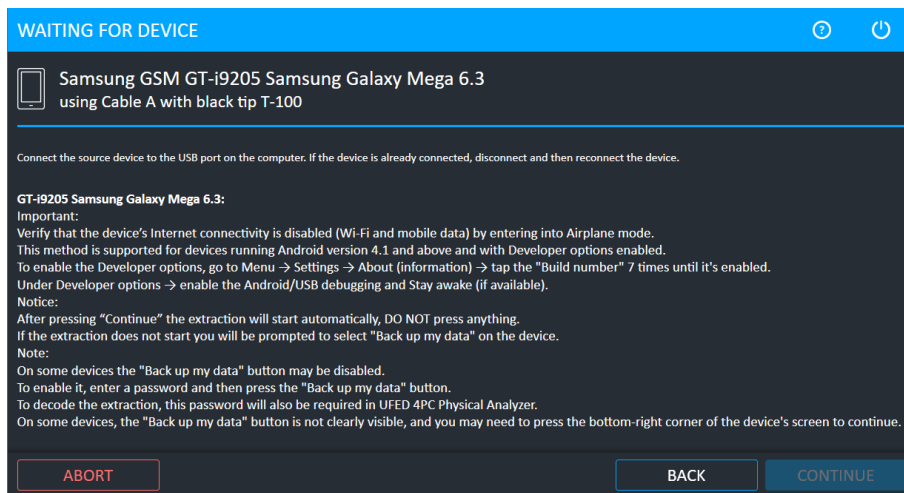
2. Click **Android Backup**.
3. Select the extraction location.



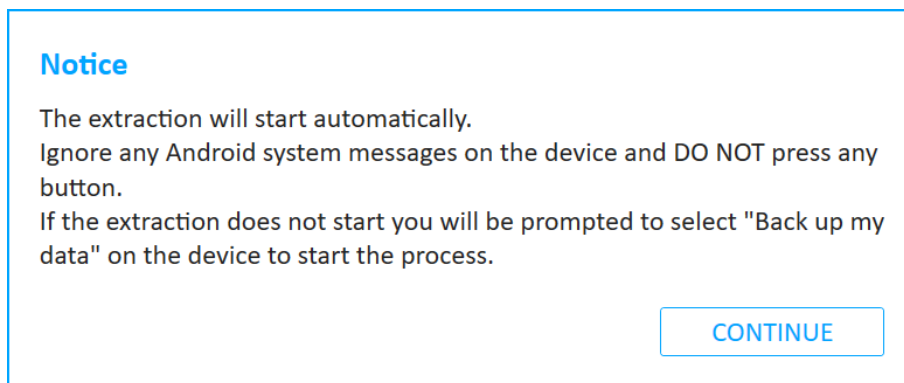
For information on using optional timeframe and party filters, refer to the *Overview Guide*.

4. Click **Continue**.

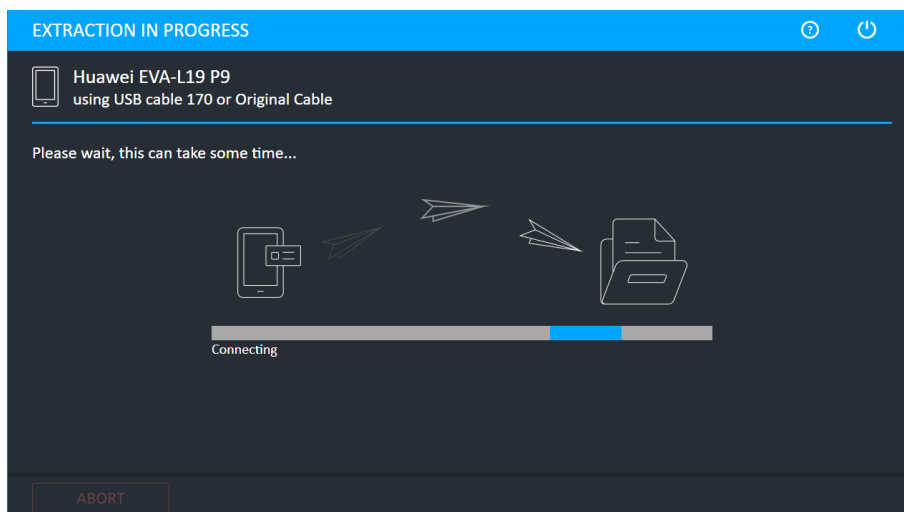
The Waiting for Device screen appears.



5. Connect the source device to the USB port. If the device is already connected, disconnect and then reconnect the device.
6. Click **Continue**. The following window appears.



7. Click **Continue** and if required select **Backup my data** on the device. The extraction begins.



The following screen appears.

### Android backup

Would you like to try data extraction from a shared location?  
The system will attempt to extract data from the device's internal storage and memory card and will take additional time.

NO

YES

8. Click **No** if you do not want to extract data from a shared location. Click **Yes** if you want to try extract data from a shared location. With a shared location, Cellebrite UFED/Responder extracts all the applications (native and non-native) that reside on the device, as well as data from the device's internal storage and memory card (images, videos, etc.), which takes additional time.

The following screen appears.

### Device Instructions

#### GT-I9205 Samsung Galaxy Mega 6.3:

Please return the Screen timeout to its original settings:

Menu (Apps) → Settings → My Device → Display → Screen timeout.

or

Menu (Apps) → Settings → Display → Screen timeout.

or

Menu (Apps) → Settings → Display → Sleep.

OK

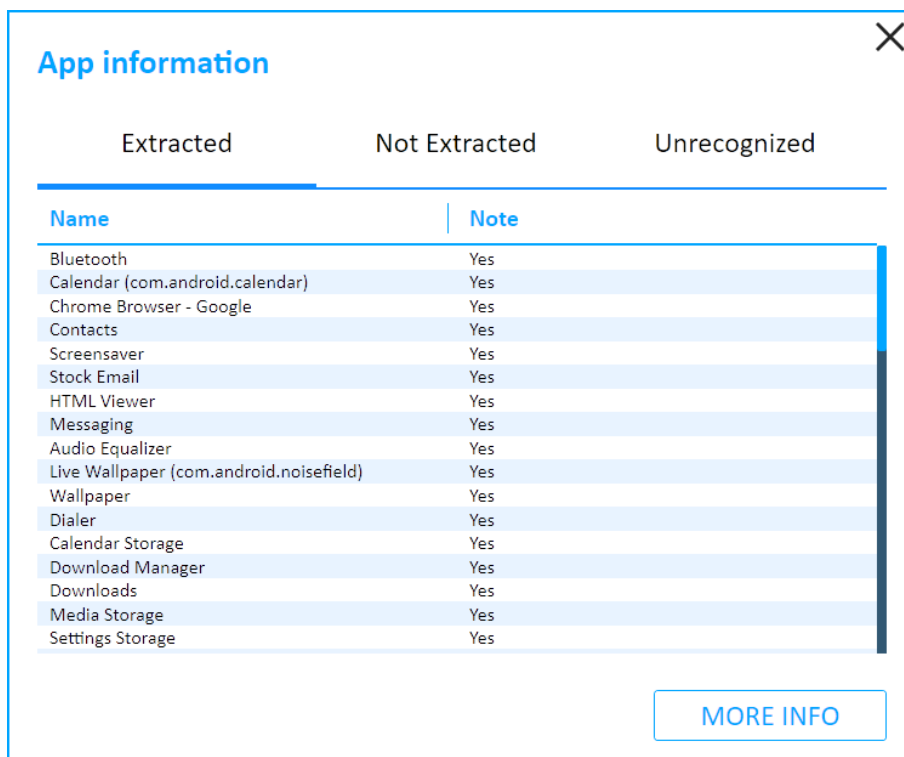
9. Follow the instructions and click OK.

When the extraction completes the Extraction summary window appears.

### 4.2.1. Extracted apps

The App information window can be displayed by clicking the **Extracted Apps** button after the File system Android backup extraction completes.

It displays the apps extraction status for the device. Apps that were extracted are listed under "Extracted". These apps will be decrypted in Physical Analyzer. Apps that could not be extracted are listed under "Not Extracted" and indicates the reason the apps were not extracted. The Notes indicate if another extraction method is applicable. Unrecognized apps and their status are listed under "Unrecognized". This list contains files that could not be mapped by the system and exist for extraction results verification. To obtain more information about these files it is recommended to do an Internet search for the file names. An example is displayed next.





### 4.3. Android backup APK downgrade

This method extracts application data using Android backup. It supports Android devices with version 4.1 and later. During the process, the selected application version (\*.apk file) is temporary downgraded to an earlier version, so that the data can be extracted. The current version is restored at the end of the extraction process. The potential risk in this method relates to the downgrading and then restoration of the app version.



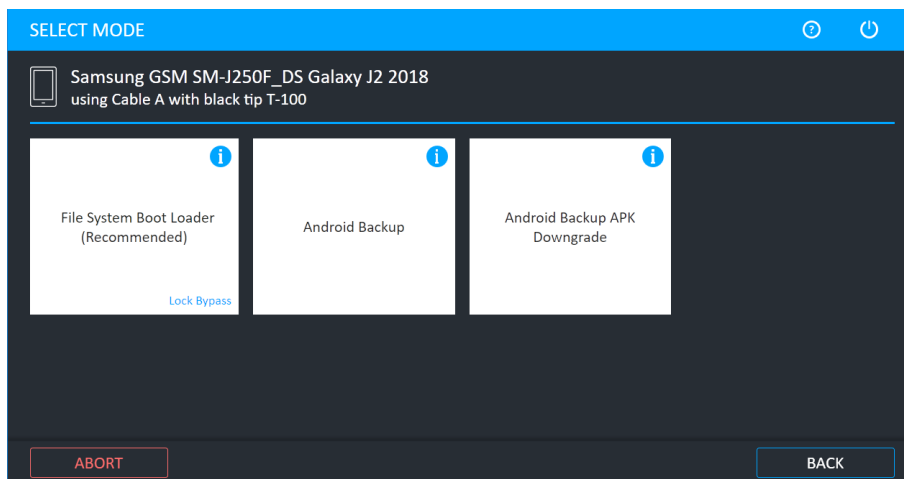
The Android Backup APK Downgrade method should be used only as a last resort after other extraction methods have been exhausted (including JTAG and chip-off).



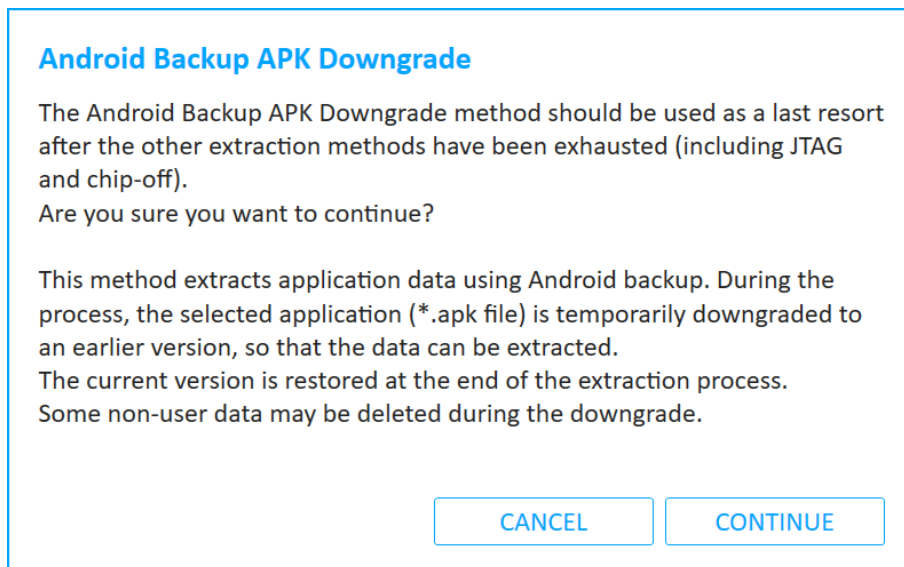
It is recommended to document the process during the extraction.

#### To extract data using Android backup APK downgrade:

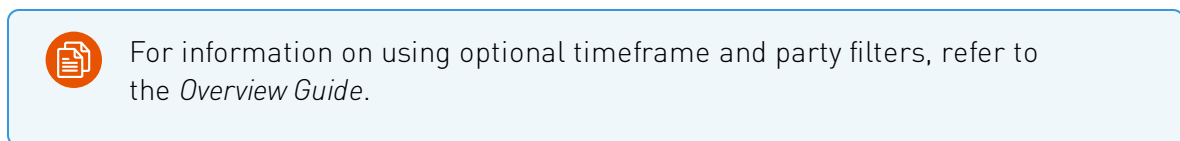
1. Click **Mobile device** and identify the device, then click **File System**. The following window appears.



2. Click **Android Backup APK Downgrade**. The following window appears.



3. Click **Continue**.



4. Select the target path. The Waiting for Device screen appears.

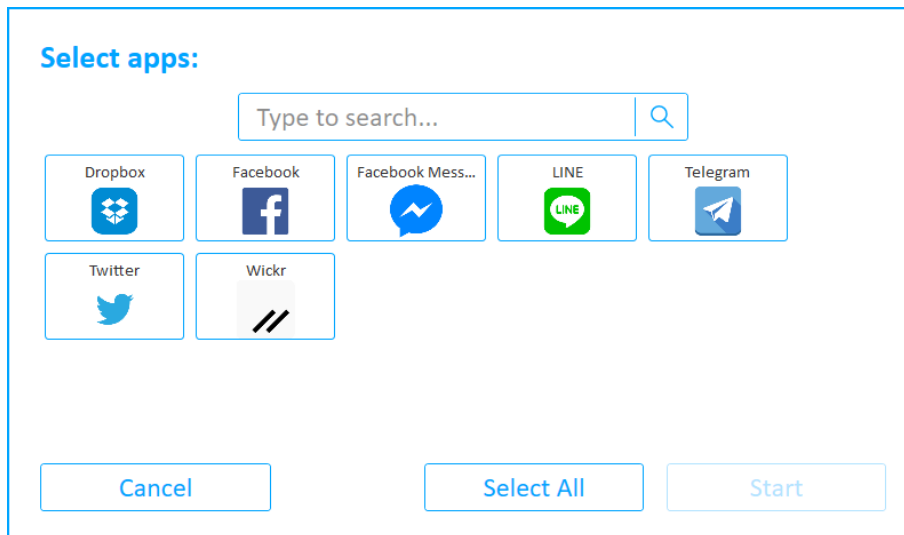


5. Connect the source device to the USB port using the specified cable. If the device is already connected, disconnect and then reconnect the device.
6. Follow the on-screen instructions for the device and then click **Continue**. The following screen appears.

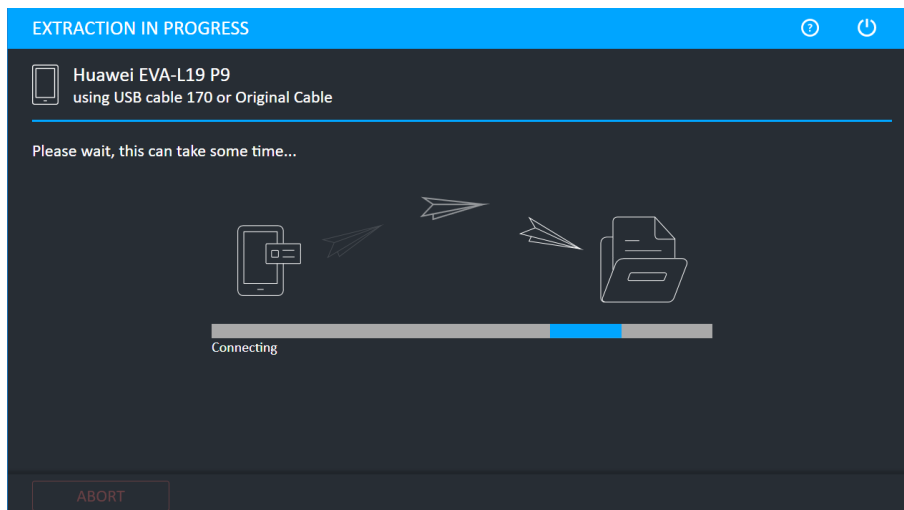


You will be notified when you are required to restart the device or to select **Backup my data** on the device. The following screen appears.

The following window appears.



7. Select the required apps (or click **Select All**) and then click **Start**. The following window appears.



8. Select **Backup my data** on the device. The following window appears.

### Android backup

Would you like to try data extraction from a shared location?

The system will attempt to extract data from the device's internal storage and memory card and will take additional time.

NO

YES

9. Click **No** if you do not want to extract data from a shared location. Click **Yes** if you want to try extract data from a shared location. With a shared location, Cellebrite UFED/Responder extracts all the applications (native and non-native) that reside on the device, as well as data from the device's internal storage and memory card (images, videos, etc.), which takes additional time.

If some app packages could not be backed up, this screen provides an indication of how many app packages were backed up successfully.

10. Click **Continue**. The following screen appears.

### Device Instructions

**GT-I9205 Samsung Galaxy Mega 6.3:**

Please return the Screen timeout to its original settings:

Menu (Apps) → Settings → My Device → Display → Screen timeout.

or

Menu (Apps) → Settings → Display → Screen timeout.

or

Menu (Apps) → Settings → Display → Sleep.

OK

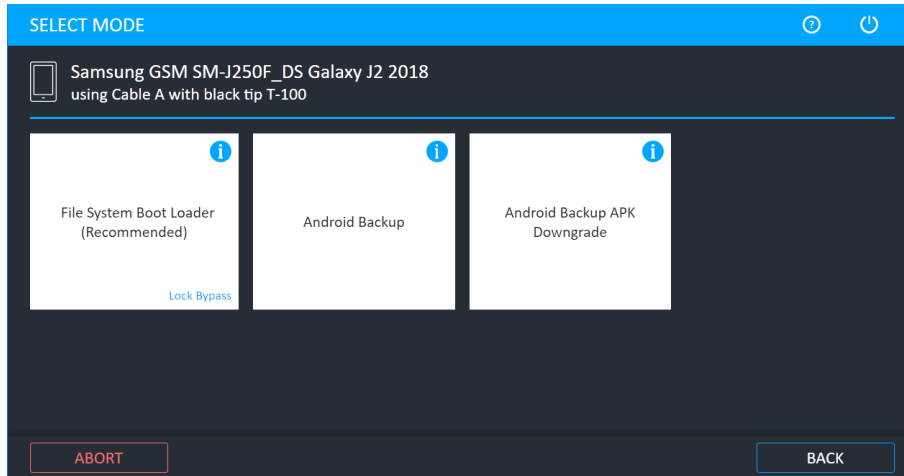
11. Follow the instructions and click OK. The Extraction summary window appears.

### 4.3.1. Android backup APK downgrade - Manual installation

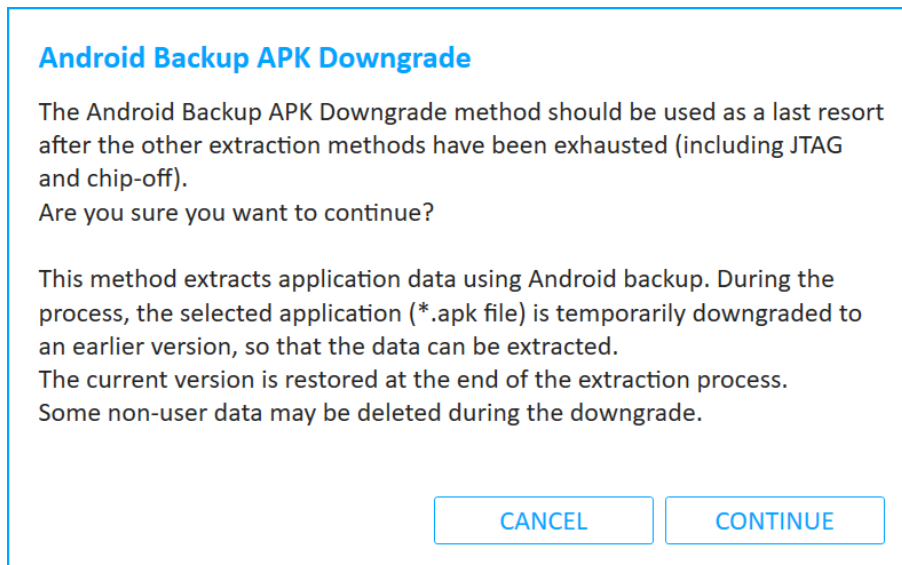
Manually intervene during the APK downgrade process to overcome installation issues where the device is not compatible.

To extract data using Android backup APK downgrade by manually installing the apps:

1. Click **Mobile device** and identify the device, then click **File System**. The following window appears.



2. Click **Android Backup APK Downgrade**. The following window appears.

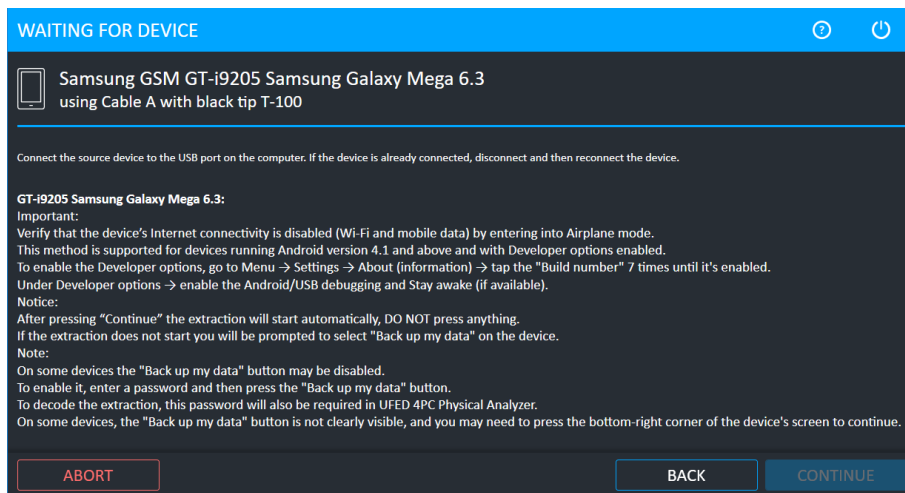


3. Click **Continue**.

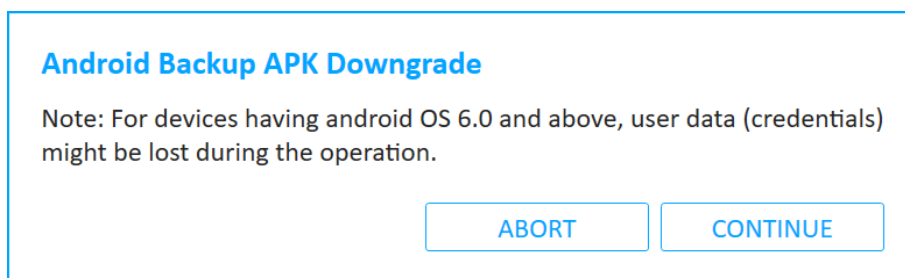


For information on using optional timeframe and party filters, refer to the *Overview Guide*.

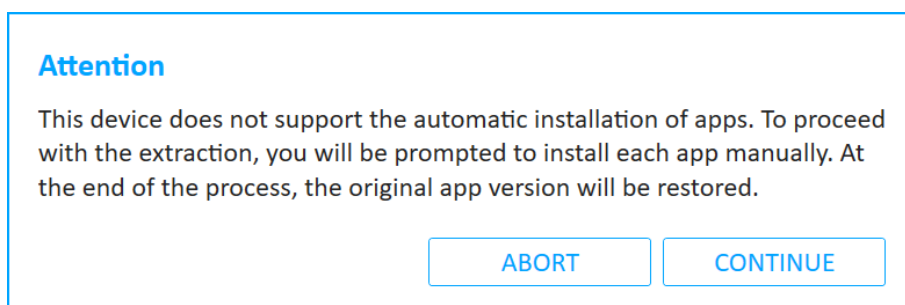
4. Select the target path. The Waiting for Device screen appears.



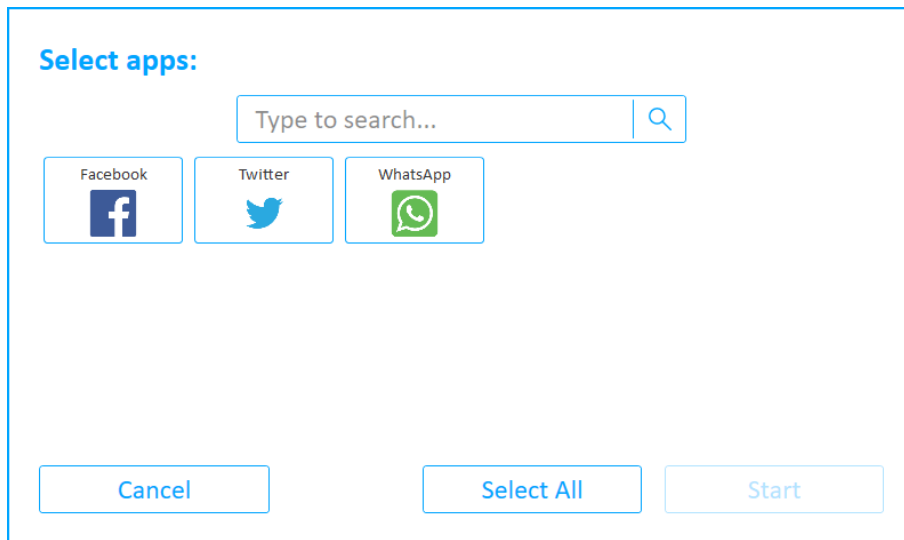
5. Connect the source device to the USB port using the specified cable. If the device is already connected, disconnect and then reconnect the device.
6. Follow the on-screen instructions for the device and then click **Continue**. The following screen appears.



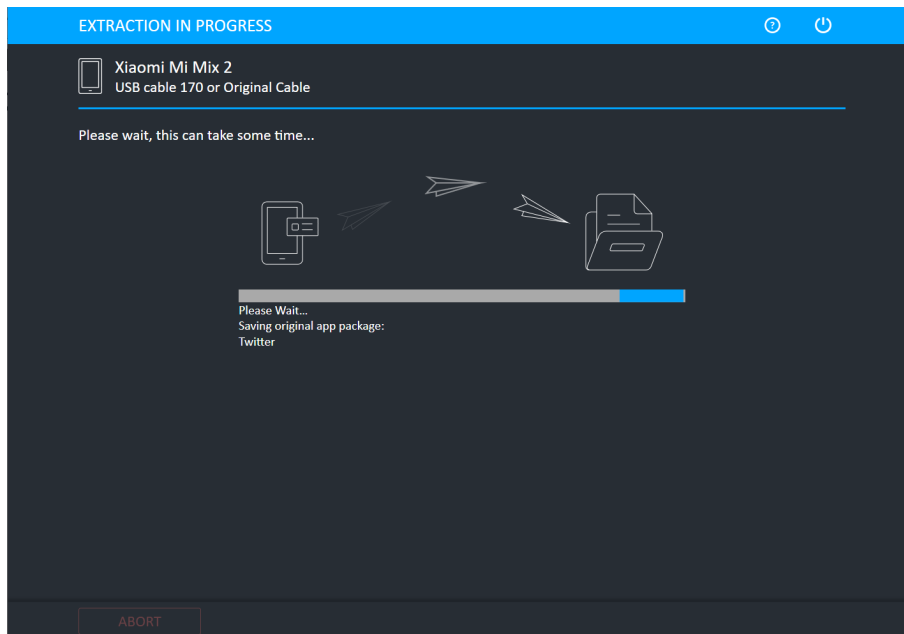
7. Click **Continue**.



8. This notification appears on devices that do not support automatic installation of apps. You will be prompted to install the apps manually. Click **Continue**.  
The following window appears.



9. Select the required apps (or click **Select All**) and then click **Start**. The following window appears.



The following window appears.



### Manual installation required

You need to manually install the app (APK file). Go to File manager (also called file explorer, my files etc.) and install the last APK file under All files/ storage called "Install\_Me.apk".

These instructions are repeated twice for each app that requires manual installation (first the app is downgraded then the original app is restored).

#### Notes:

- After installing an app press "Done" on the source device's screen (do not press "Open").
- Go back to the File manager screen after every installation so that you can install other required apps.
- In some devices you will be prompted to grant "Install unknown apps" permissions in the File manager.

CONTINUE

10. Manually install the APK file. Go to the File Manager (also called File Explorer, My Files, Mi File Manager etc.) on the source device and install the "Install\_Me.apk" under All files or Storage. The icon of the app appears next to the "Install\_Me.apk".
11. After installing the app, press **Done** on the source device's screen (do not press **Open**).
12. Go back to the File Manager screen after every installation so that you can install all the required apps.
13. Click **Continue**.



You will be notified when to select **Backup my data** on the device to continue with the Android Backup process. For more information, see [Android backup APK downgrade \(on page 45\)](#).

## 4.4. Vendor backup

### 4.4.1. LG backup

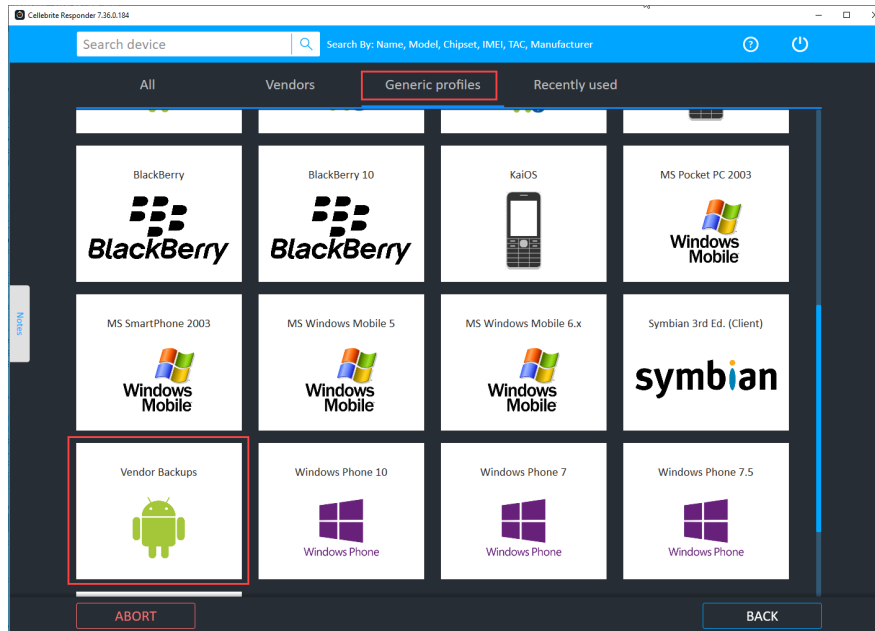
LG vendor backup allows you to extract user data that includes:

- » **Personal data** - contacts, text messages, call history, etc.
- » **Media data** - images, videos, audio, and documents
- » **Installed applications data** - LG settings, etc.

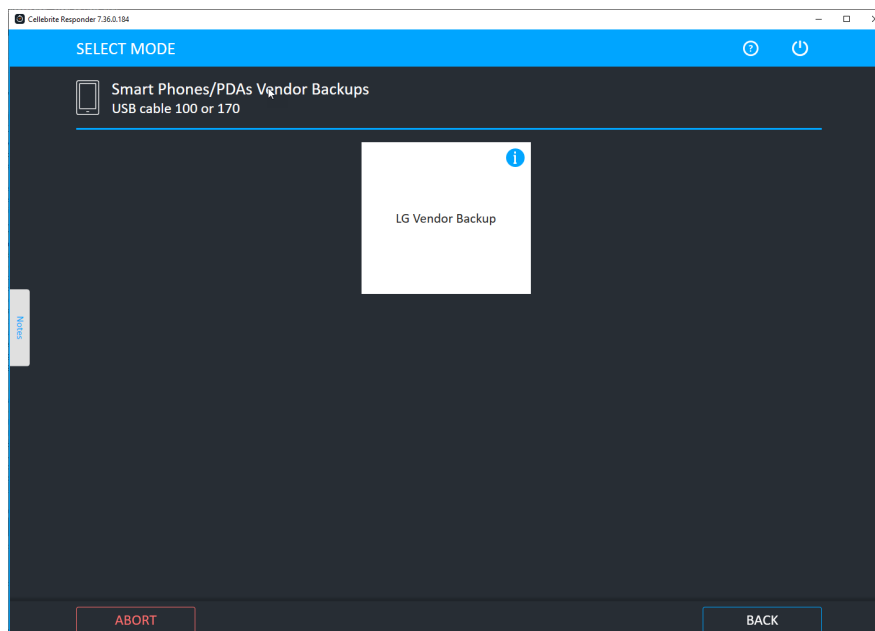
This method supports all LG devices running on Android OS versions 5.x and higher. The extraction is first saved on the device's internal memory and then saved on the target.

## To extract data using LG backup:

1. Click on **Mobile device**.
2. Enter case details and click **Continue**.
3. Click **Browse devices**.
4. Under **Generic profiles** tab, select **Vendor backups**.

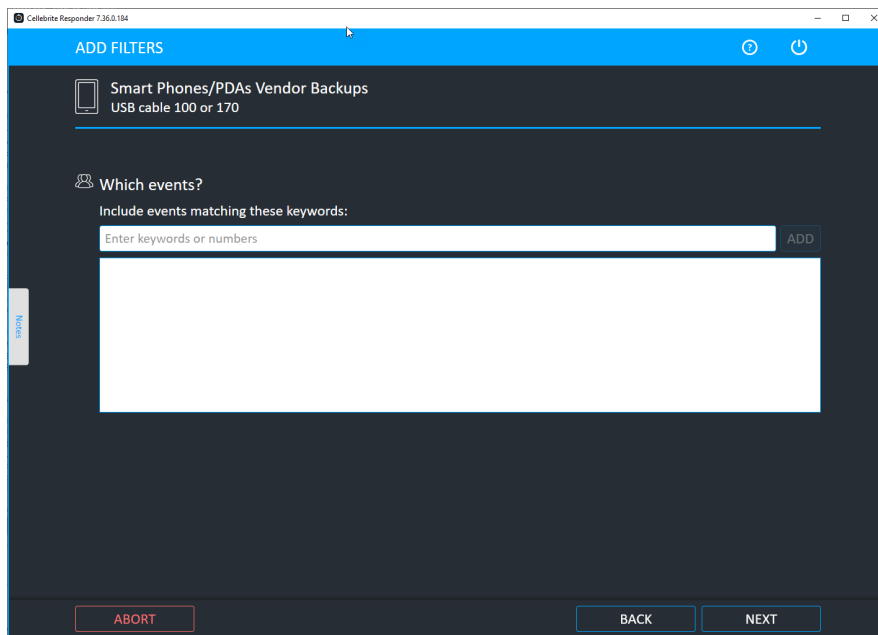


5. Click **File system**.
6. Click **LG vendor backup**.

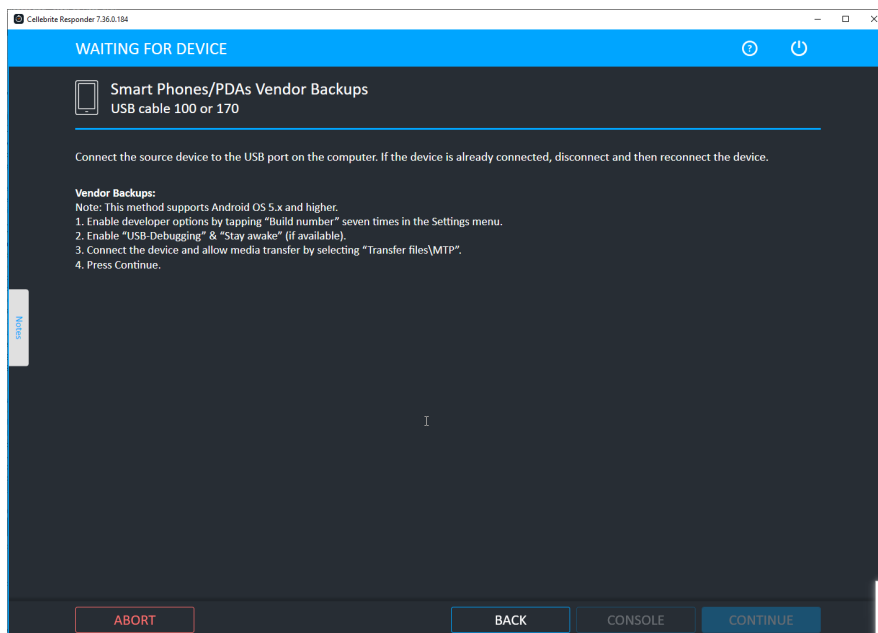


7. Enter keywords to include relevant events.

8. Click **Next**.



9. Connect the device.



## 4.5. Selective file system extraction

Selective extraction is part of the full file system extraction. It extracts all relevant app data located under the root directory. The app data includes folders and files associated with the app such as databases, APKs, images, and keys. Selective extraction takes less time to complete compared to a full file system extraction and enables you to only select the apps that are required.

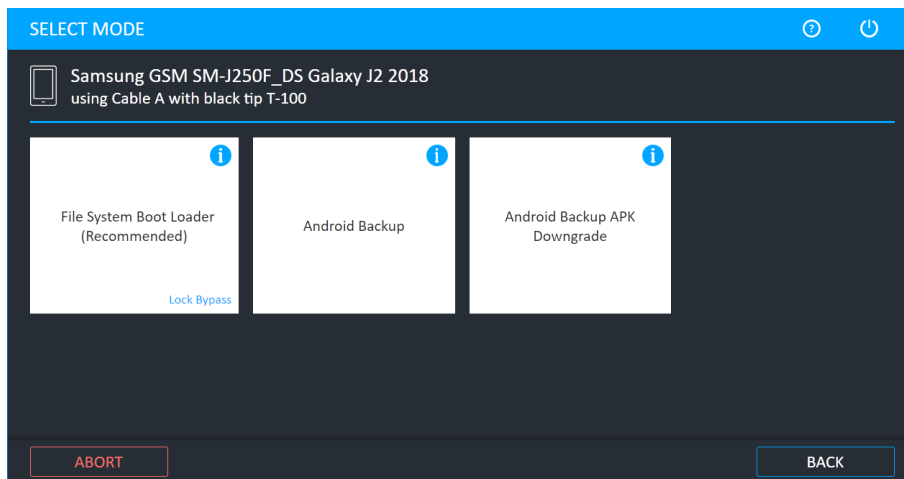
Selective extraction is currently supported for EDL Decrypting Bootloader, Samsung Qualcomm Decrypting Bootloader and Huawei Decrypting Bootloader methods.



Selective extraction does not extract data from unallocated space. Use one of the Physical extraction methods instead.

### To extract data using Selective file system extraction:

1. Click **Mobile device** and identify the device, then click **File System**.

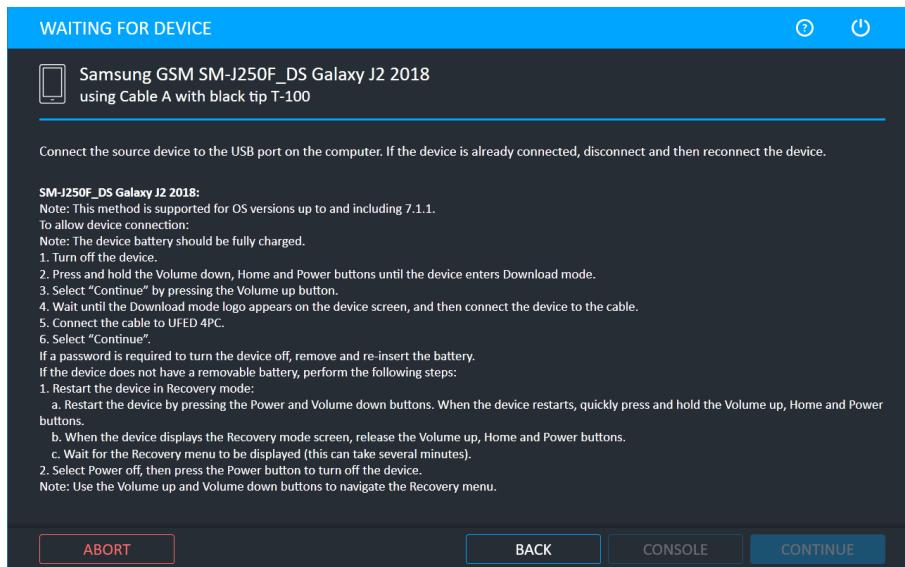


2. Click **File System Boot Loader**.

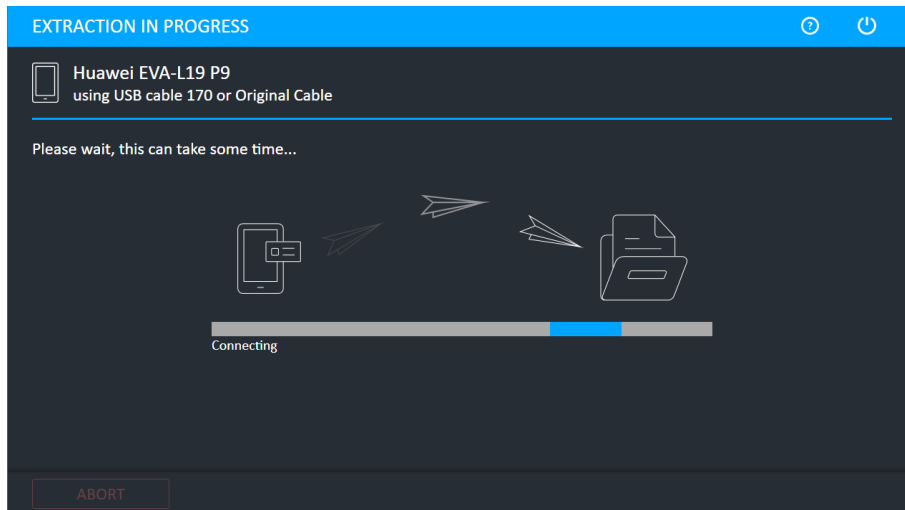


For information on using optional timeframe and party filters, refer to the *Overview Guide*.

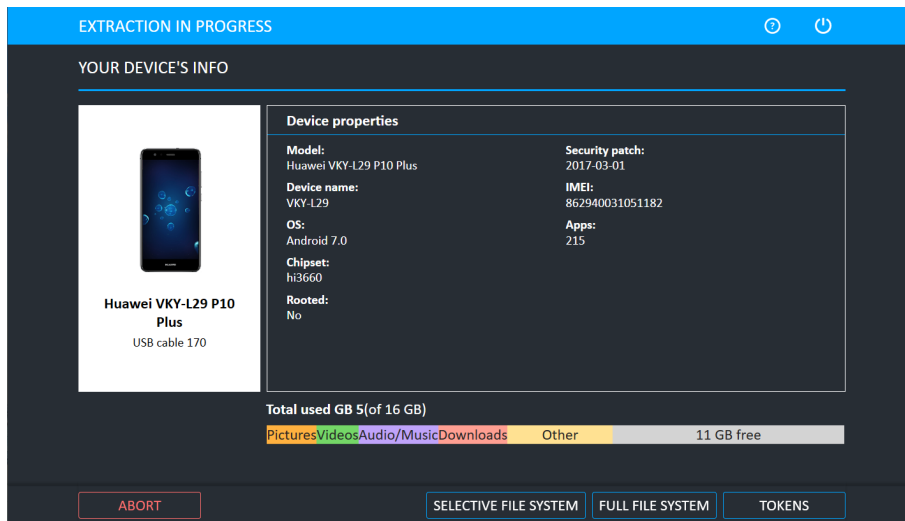
3. Select the extraction location.
4. Click **Continue**. The Waiting for Device screen appears.



5. Connect the source device to the USB port. If the device is already connected, disconnect and then reconnect the device.
6. Click **Continue**. The following window appears.



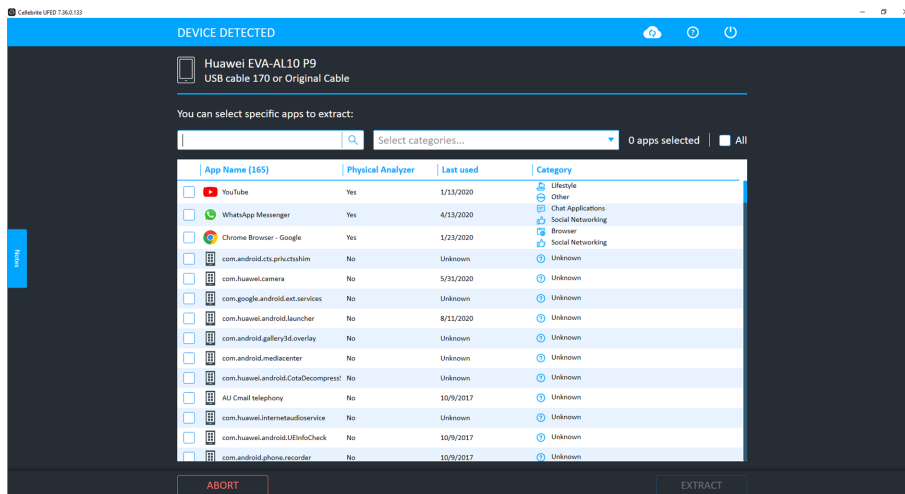
The following window appears.



This window displays the device properties such as model, device name, OS, chipset, whether the device is rooted, date security patch installed, IMEA, and the number of installed apps, and what data is on a device including storage volume, data types, volume of storage per data type, and free data. Click one of the following options:

- » **Selective File System:** The Selective extraction takes less time to complete and enables you to only select the required apps to extract.
- » **Full File System:** Full file system extraction including all apps and tokens.
- » **Tokens:** Retrieve data from cloud sources. Upon extraction and decoding, create the account package in Physical Analyzer and upload it into UFED Cloud.

A Selective file system extraction example is displayed next.



7. Select the required apps and the click **Extract**. The Extraction Summary window appears.



You can search for apps by category from the Select categories list.

## 5. Physical extraction

The **Physical Extraction** function enables you to perform a physical bit-for-bit image of the source device memory to a removable storage device or PC.

Physical extractions include the following:

[Performing a physical extraction \(on page 60\)](#)

[ADB rooted \(on page 63\)](#)

[Advanced ADB \(on page 65\)](#)

[Boot loader \(FW flashing\) \(on page 82\)](#)

[Decrypting boot loader \(on page 85\)](#)

[Forensic recovery partition \(on page 87\)](#)

[Smart ADB \(on page 91\)](#)



UFED now provides a notification if advanced forensic capabilities are available via Cellebrite Advanced Services for a growing range of supported Android and iOS devices. To learn more refer to:  
<https://www.cellebrite.com/en/services/advanced-unlocking-services/>

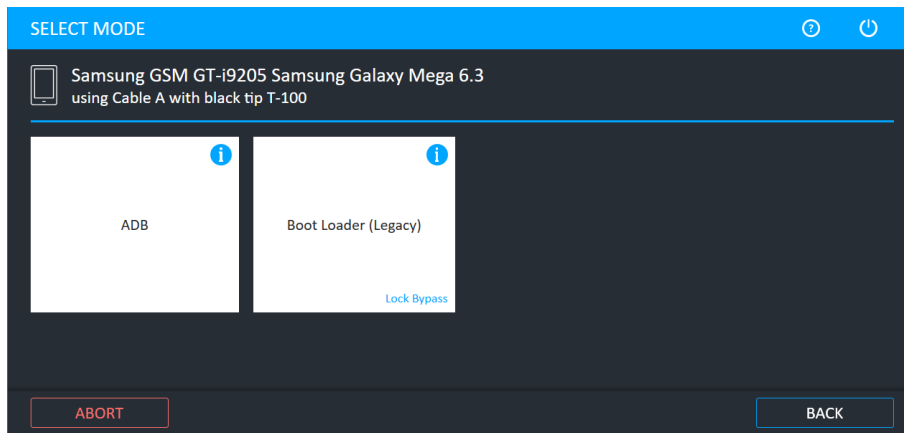


Lock Bypass is displayed if the physical extraction method can bypass the user lock of the device.

## 6.1. Performing a physical extraction

1. Click **Mobile device** and identify the device, then click **Physical**.

The Select Mode screen appears.



2. Click **ADB** or **Boot Loader (Legacy)**.

- » **ADB:** Android Debug Bridge (ADB) is a built-in communication mechanism that allows device debugging. With this extraction method, it is possible to perform a physical or file system extraction, provided that the device's USB debugging option is enabled. If the device is not already rooted, UFED will attempt to temporarily gain the permissions required for the extraction. In some cases, data from a memory card will be extracted; however, the recommended method is to read the card with an external memory card reader.
- » **Boot Loader:** An extraction method that performs a physical extraction when the device is in bootloader mode. With this extraction, the operating system is not running, so the device cannot connect to the mobile network. It bypasses any user lock and is forensically sound. The bootloader extraction does not support extractions from a memory card.

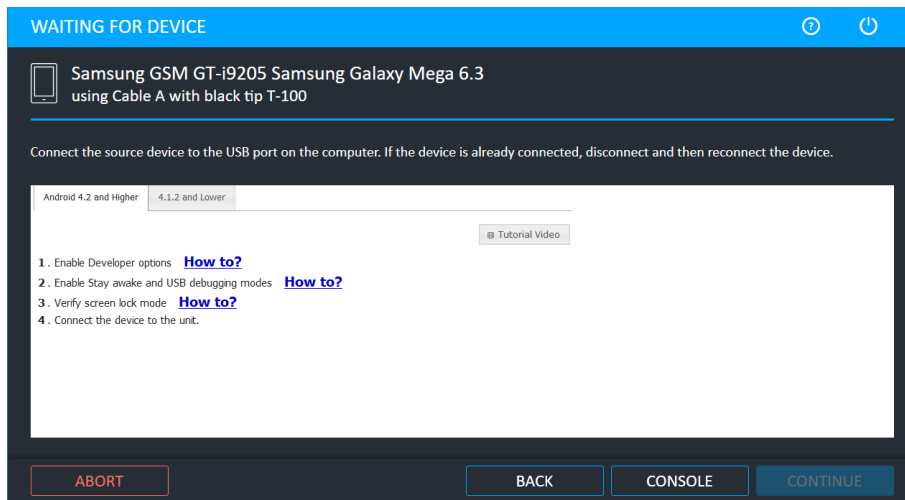


For information on using optional timeframe and party filters, refer to the *Overview Guide*.

The Select Extraction Location screen appears.

3. Click **Next**.





4. Do the following:
  - » Select the correct cable and tip for the mobile device based on the instruction on the screen.
  - » Change the device settings according to the instructions.
5. Click **Continue**. The Extraction in Progress screen appears.



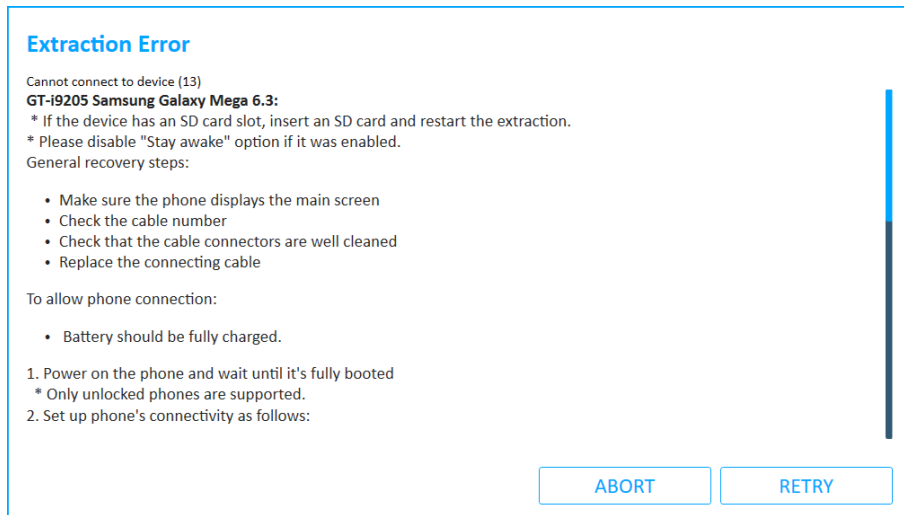
6. Follow any on-screen instructions.



For some devices, an estimation of the time the extraction will take is displayed: For example, Blackberry, Nokia BB5, QCP (SamM550, LgEmergency, LgP0), Android, (generic and SPF), SpreadTrum, Samsung GSM (MTK, LGInfinion, and BCM2133), and Palm.

## If the system cannot connect to the device:

The following window appears with an error message.



» Follow the instructions on the screen and click **Retry**.

### 6.1.1. The Physical extraction folder

At the end of the physical extraction process, the extracted data is saved in the location you selected during the physical extraction process. See step 5 of Performing a Physical Extraction.



The extracted data folder is named "Physical" with the selected device name and the extraction operation date. For example, "Physical Samsung GSM SGH-A711 2011\_06\_12 (001)"

The extracted data folder contains:

- » Binary file of the device memory.
- » UDF file containing the system extraction information, used by the Physical Analyzer application.

The extraction information can be viewed using the Physical Analyzer. You can double click on the UDF file or open it via the GUI.

## 6.2. ADB rooted

The ADB method for Android rooted devices can be used when the physical extraction method is not supported. Using the ADB method, you can perform a physical extraction from rooted Android devices. This extraction method is for pre-rooted devices only, and does not root the device. To “root” a device means to gain administrative rights on the file system.

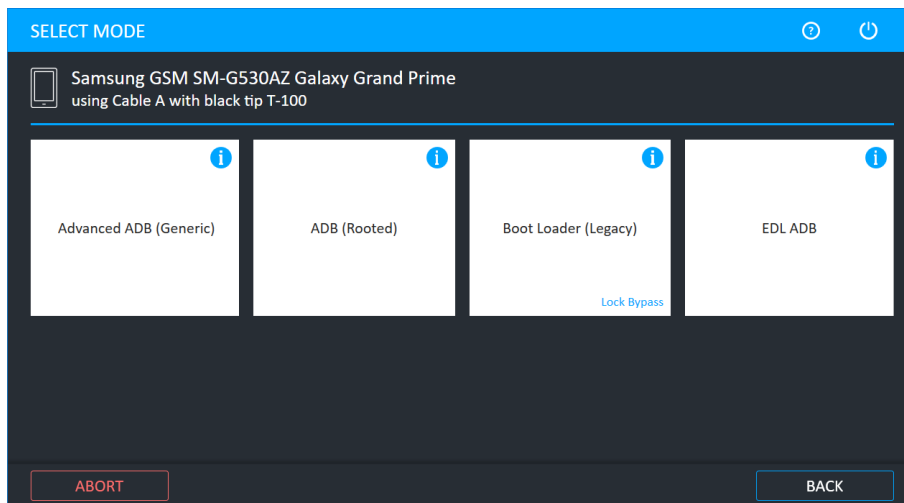


A device can be rooted as part of recovery partition or fully rooted following a rooting procedure. It does not suggest that you should root the device, however, if there is no other option, you can use this method.

### To perform a physical extraction for a rooted Android device:

1. Click **Mobile device** and identify the device, then click **Physical**.

The Select Mode screen appears:



2. Click **ADB (Rooted)**.

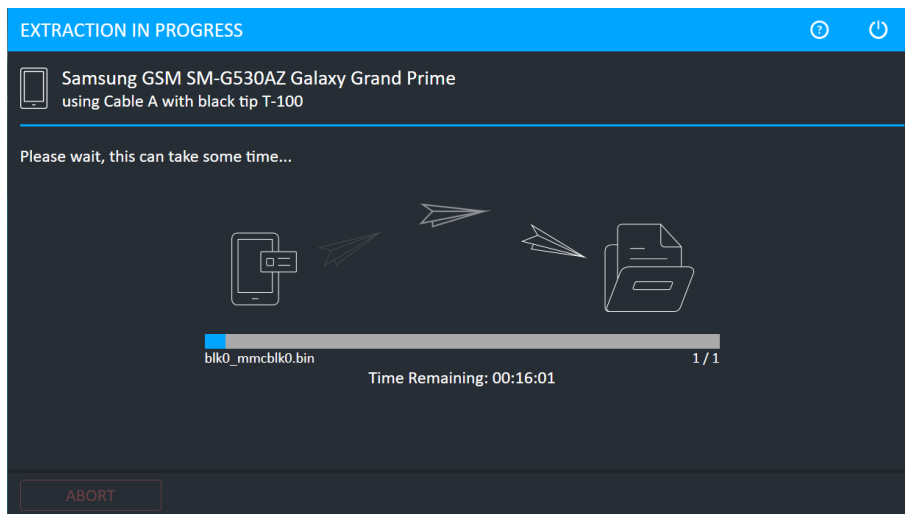


For information on using optional timeframe and party filters, refer to the *Overview Guide*.

The Select Extraction Location screen appears.

3. Click **Next**. The following window appears.
4. Do the following:
  - » Select the correct cable and tip for the mobile device based on the instruction on the screen.
  - » Change the device settings according to the instructions.
5. Click **Continue**.

The Extraction in Progress screen appears.



6. Follow any on-screen instructions.

## 6.3. Advanced ADB

Advanced ADB extraction enables physical extraction of data from additional devices. This method supports devices with Android operating systems up to version 7.1, on devices with a security patch level up to November 2016, including Galaxy S7, Galaxy Note 5, LG G5, V20, and Nexus devices.



Due to the widely fragmented variance in Android devices, exceptions may apply.



To avoid any interruptions during the extraction, the device must be placed in Airplane mode.

### Before performing an Advanced ADB extraction:

1. Make sure the source device is fully charged.
2. Prepare a target storage device on which to save the extraction file. This target can be either a USB mass storage device (connected via OTG cable 501 or 508), or an SD memory card.
  - » The target storage device must be a FAT32/vFAT/exFAT format and have sufficient space for the extraction.
  - » If a USB drive is selected for the target storage, make sure you have an available OTG cable for the extraction: OTG cable 501 (micro USB connector) or cable 508 (type C connector). OTG cable example:



- » If an SD card is selected for the target storage, place it in the Android device now.



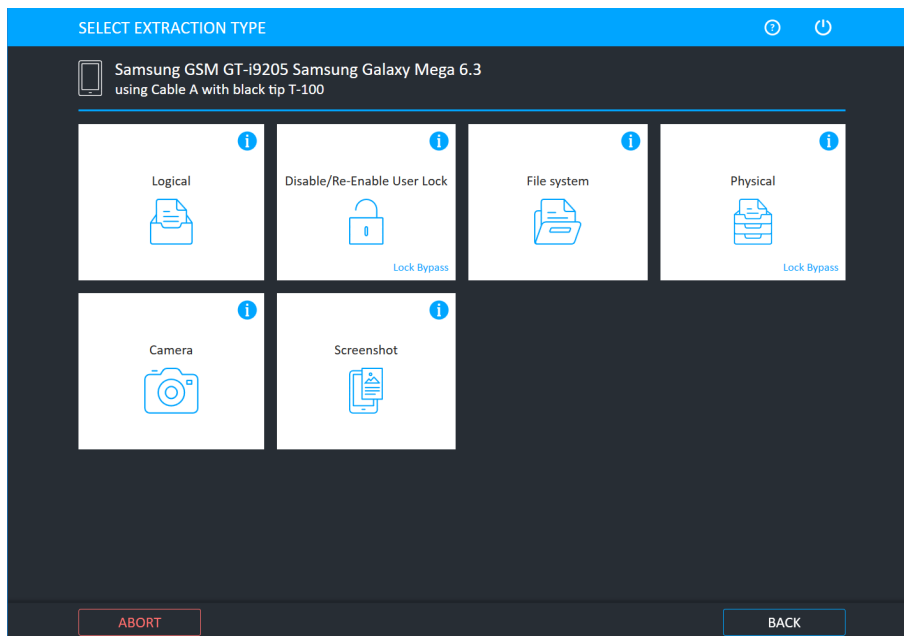
The SD card must be blank and not contain any case evidence.



If the card port location is under the device's battery, restarting may re-lock a device that was locked before. Therefore, for devices with OTG support, we recommend using a USB drive for the target storage.

## To perform an Advanced ADB extraction:

1. From the Home screen, detect the relevant device automatically. The following window appears.



If the relevant model is not listed, browse manually for a generic Android model. See [Generic model \(on page 73\)](#).

2. Click **Physical**.  
The Select Mode screen appears.
3. Click **Advanced ADB**.



For information on using optional timeframe and party filters, refer to the *Overview Guide*.

4. Follow the instructions to set up device connectivity.
5. On the source device, perform the following steps:
  - a. On an Android OS 4.3 and above, Go to **Menu (Apps) > Settings (More) > Security** and clear the Verify apps setting. Approve any pop-ups that may appear.
  - b. Go to **Menu (Apps) > Settings (More) > About (Software information) > More**, and tap the Build number 7 times until developer options are enabled.
  - c. Go to **Development settings** and enable USB debugging.
  - d. Connect the source device to the cable described in UFED.
  - e. A notification is added to the notification drop down. Allow MTP/PTP on the device.

6. On the UFED screen, click **Continue**. The following window appears.

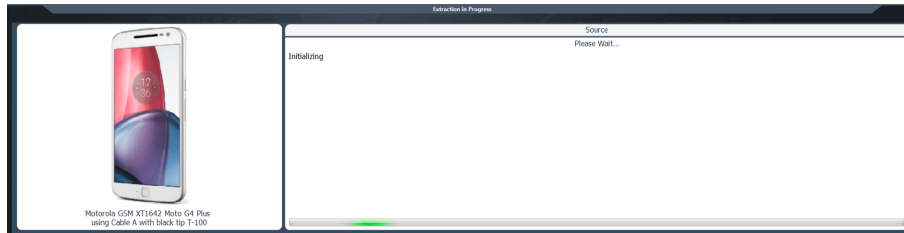
**Warning**

Before you select the target storage:  
If the target storage is an SD card, place it in the device now.  
Reminder: Restarting may re-lock the device. For this reason a USB drive is recommended for the target storage.

If the target device is not recognized by the Android device click "Help with storage format"

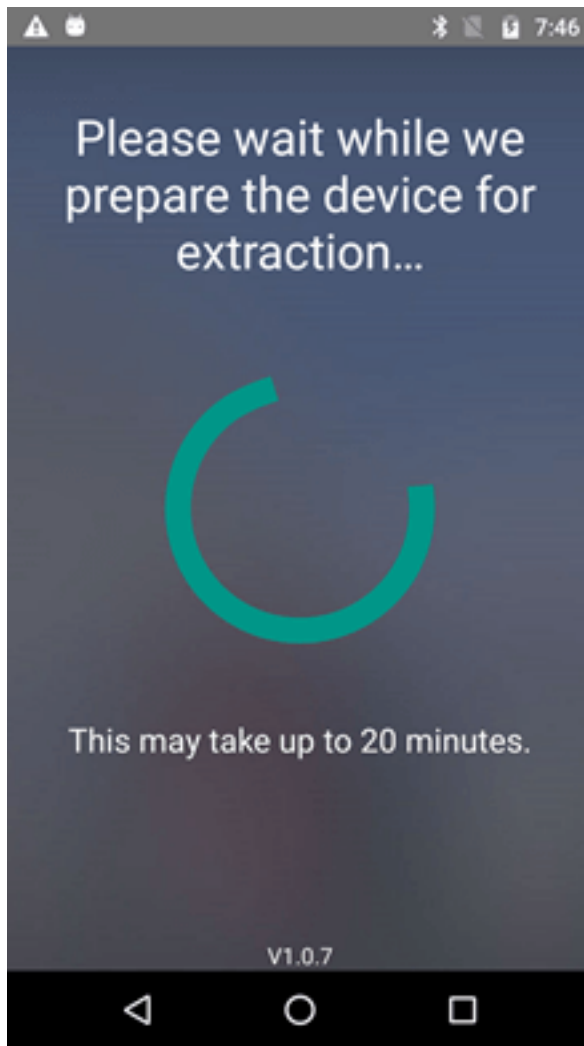
SD CARD WAS INSERTEDMASS STORAGEHELP WITH STORAGE FORMAT

7. Click the relevant target storage. The following window appears.



If requested, you should only approve the installation of apps.

UFED is installing the extraction app and attempting to temporarily gain the permissions required for the extraction. This stage can take approximately 20 minutes. During this process, the device screen appears.

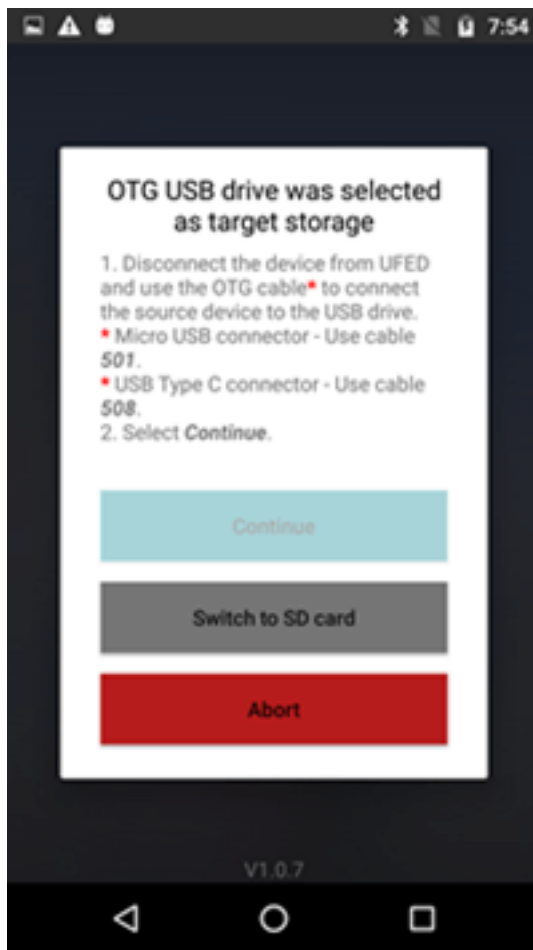


When UFED has prepared the device, a window appears indicating that the device is ready for extraction. Disconnect the device from UFED and follow the instructions on the source device.

8. Click **Continue**.
9. Follow the instructions on the Android source device's screen. For a USB drive target, continue to the following step. For an SD card target, skip to the next step.



10. If a **USB drive target** was selected, the following screen appears.



- a. Follow the on-screen instructions:
  - i. Disconnect the device from UFED.
  - ii. Use the OTG cable to connect the source device to the USB drive.

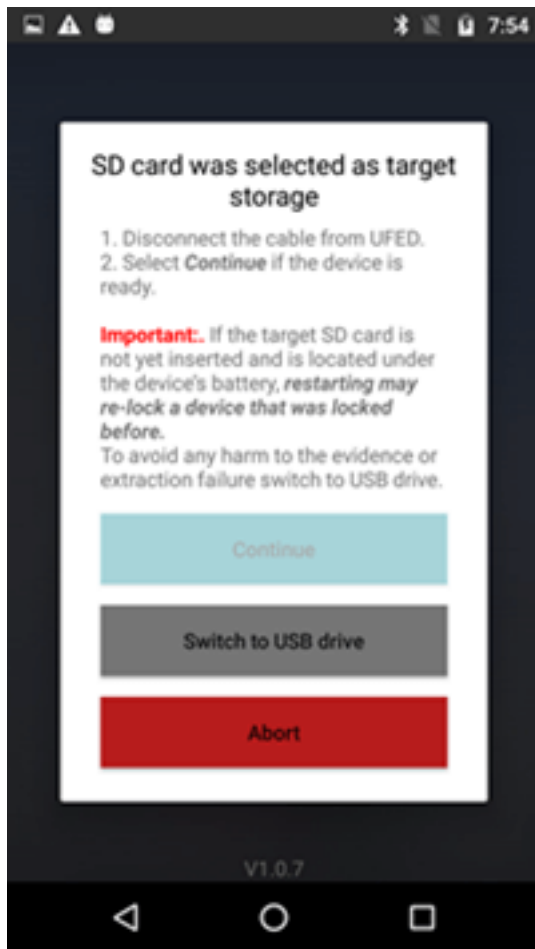


Selecting **Switch to SD card** will change the target type configuration.



Selecting **Abort** will end the extraction process and will require a device restart.

- b. Skip the SD card step.
- c. If an **SD card target** was selected, the following screen appears.



- a. Follow the on-screen instructions:
  - i. Disconnect the device from UFED.
  - ii. If the target SD card is not yet inserted and is located under the device's battery, restarting may re-lock a device that was locked before. To avoid an extraction failure (for devices with OTG support), select **Switch to USB drive**.

Reminder: This target device requires A FAT32\*/vFAT/exFAT format SD card with sufficient space for the extraction.

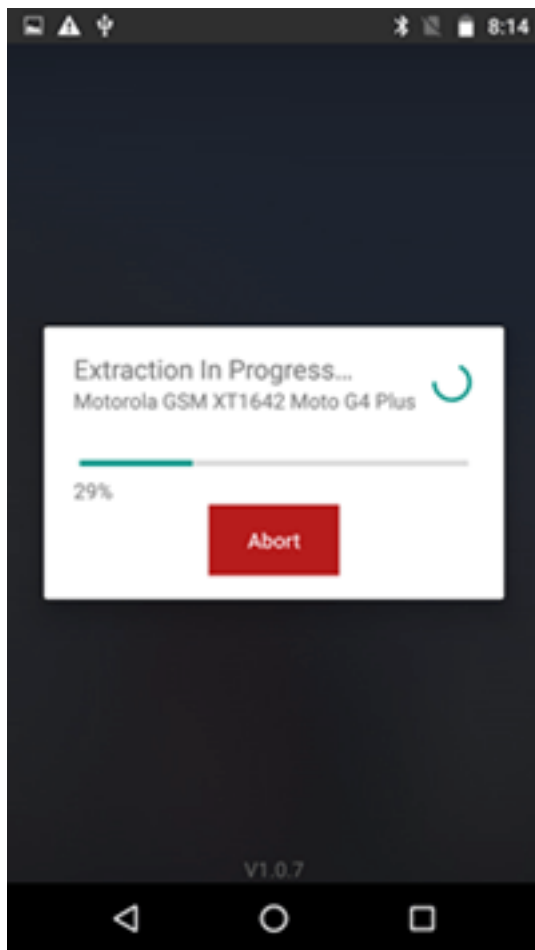


Selecting **Switch to USB drive** will change the target type configuration.

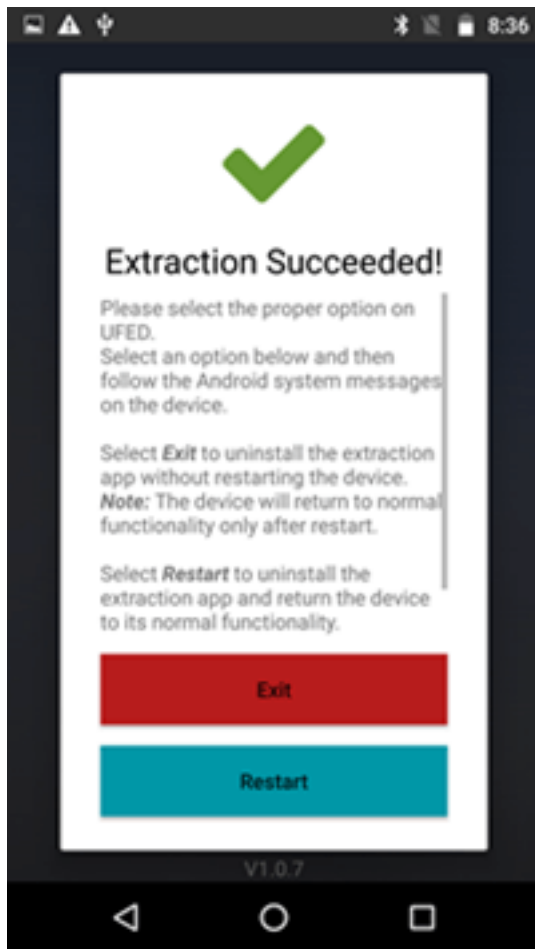


Selecting **Abort** will end the extraction process and will require a device restart.

12. Select **Continue**. The reading process begins.



When the extraction is successfully completed, the following screen appears.



13. Select **Exit** to uninstall the extraction app without restarting the device, or select **Restart** to uninstall the extraction app and return the device to its normal functionality.



Restarting may re-lock a device that was locked before.



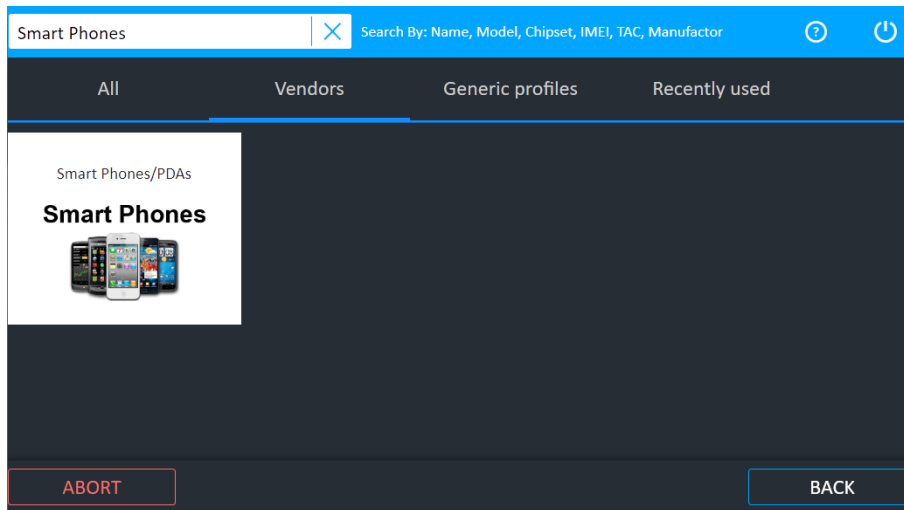
The device will only return to normal functionality after restart.

14. Return to UFED.
15. Follow the on-screen instructions on the source device. When the extraction completes click **Extraction failed**, **Extraction successful** or **Abort** to update the extraction Activity log.
16. Click the relevant extraction status to update the extraction Activity log.
17. Follow the instructions and click **Finish**.

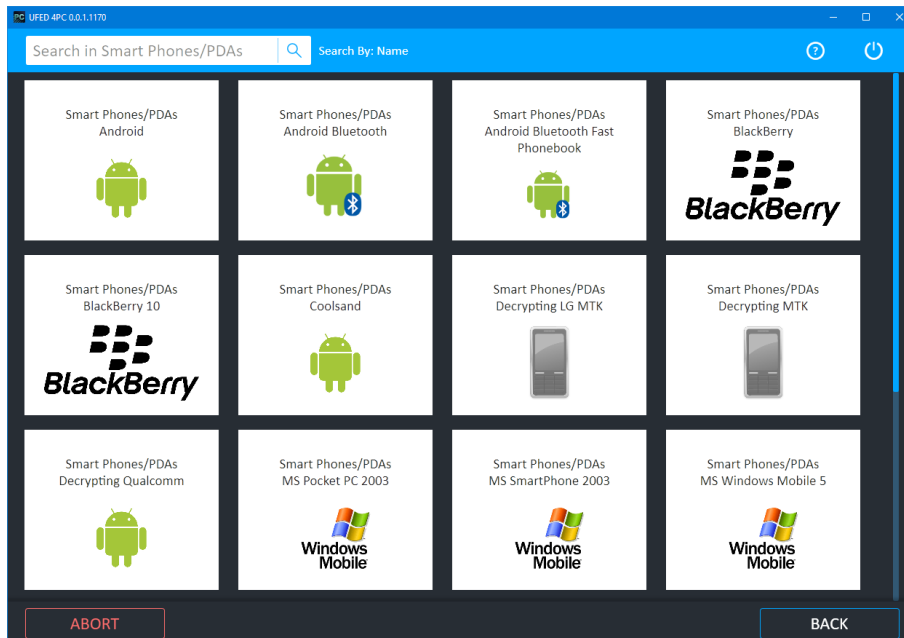
### 6.3.1. Generic model

To perform an Advanced ADB extraction:

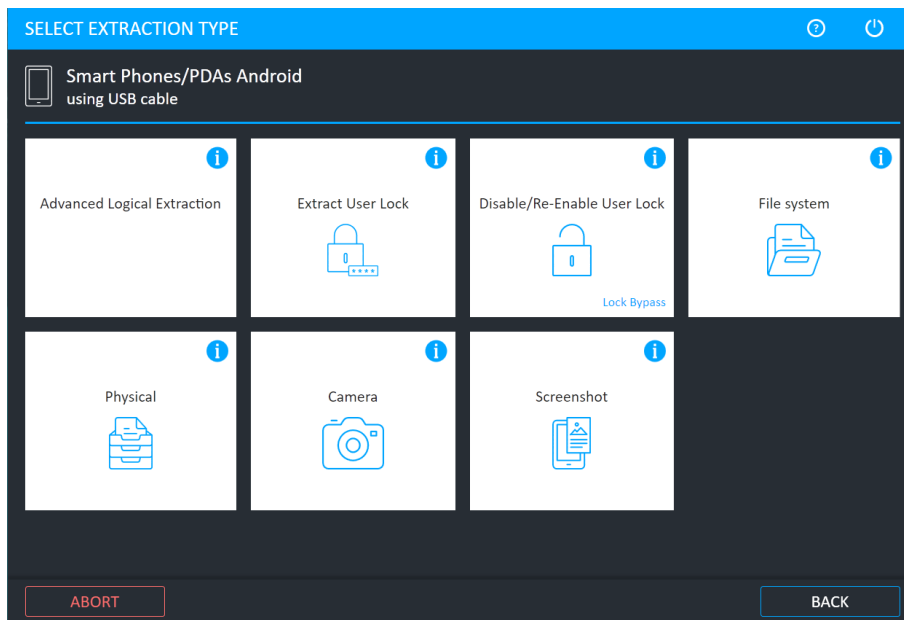
1. From the Home screen, click **Skip** > **Vendors** (tab) and search for "Smart Phones". The following window appears.



2. Click **Smart Phones**. The following window appears.



3. Click the relevant model. The following window appears.



4. Click **Physical**.
5. To continue, refer to [Advanced ADB \(on page 65\)](#).

## 6.3.2. Errors and notifications

### 6.3.2.1. Disk format error

#### Storage Format

To format the target storage you can use your Android device or your PC.

From the Android device:

SD card - Insert the SD card in the relevant slot of the Android device now.

USB drive - Connect the USB drive via the OTG cable to the Android device now.

Open the Android device notification drop-down and select the USB message  
or go to device portable storage settings and follow the instructions to erase  
and format the device.

From your PC:

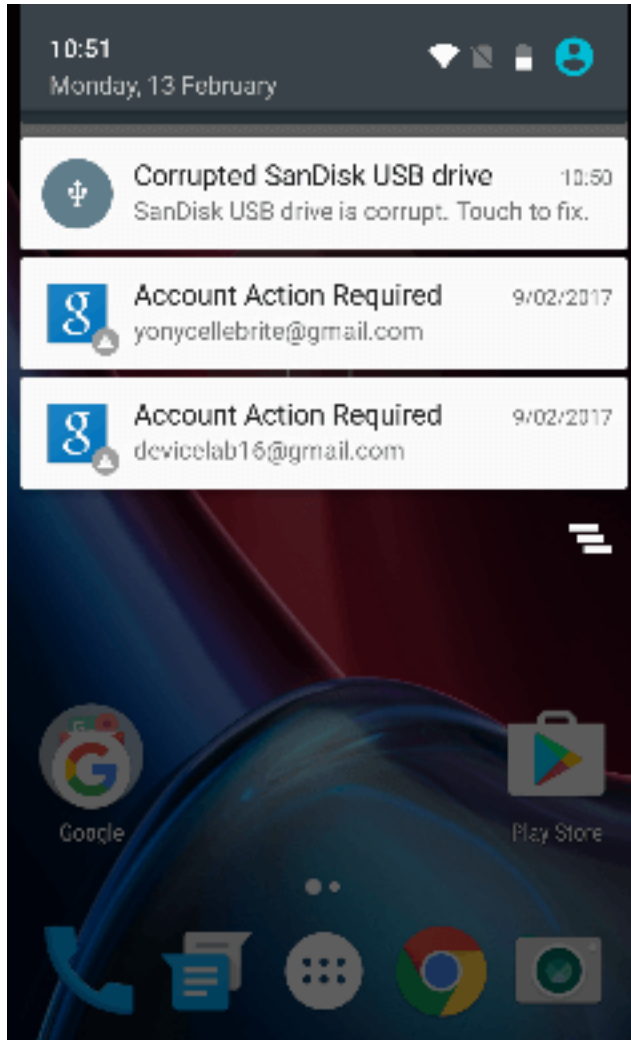
Plug the target device into your Windows PC. Right-click the storage drive and select "Format...". In the format window, under File system, select exFat. Click "Start" and complete the format process.

STORAGE IS FORMATTED

If you receive this error message, follow the instructions listed in the error message.

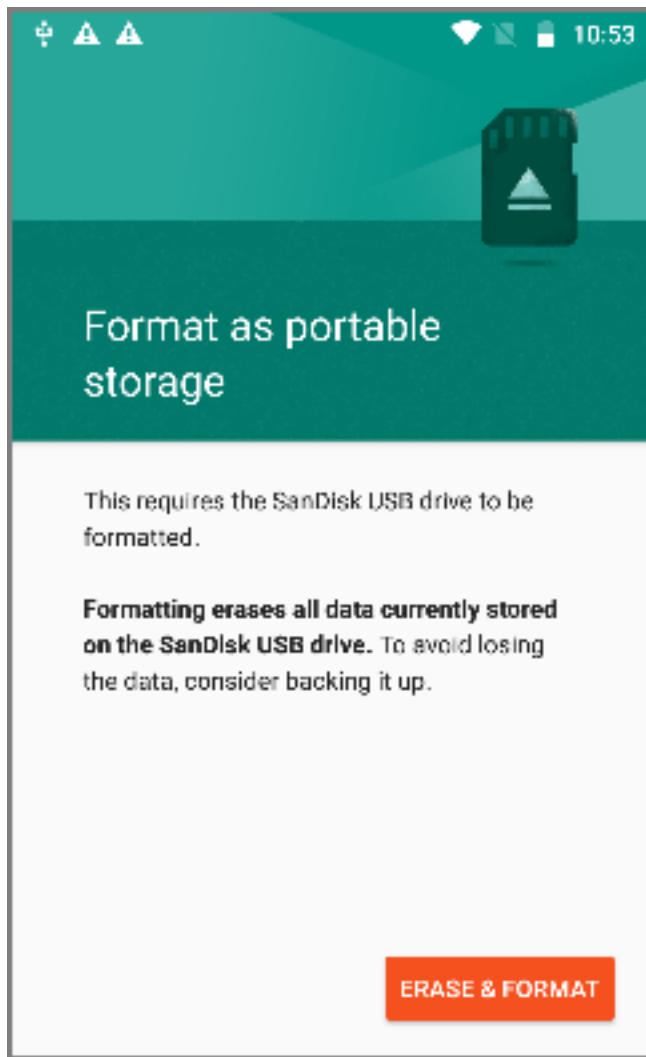
To format the storage device from the Android device:

1. Open notification.

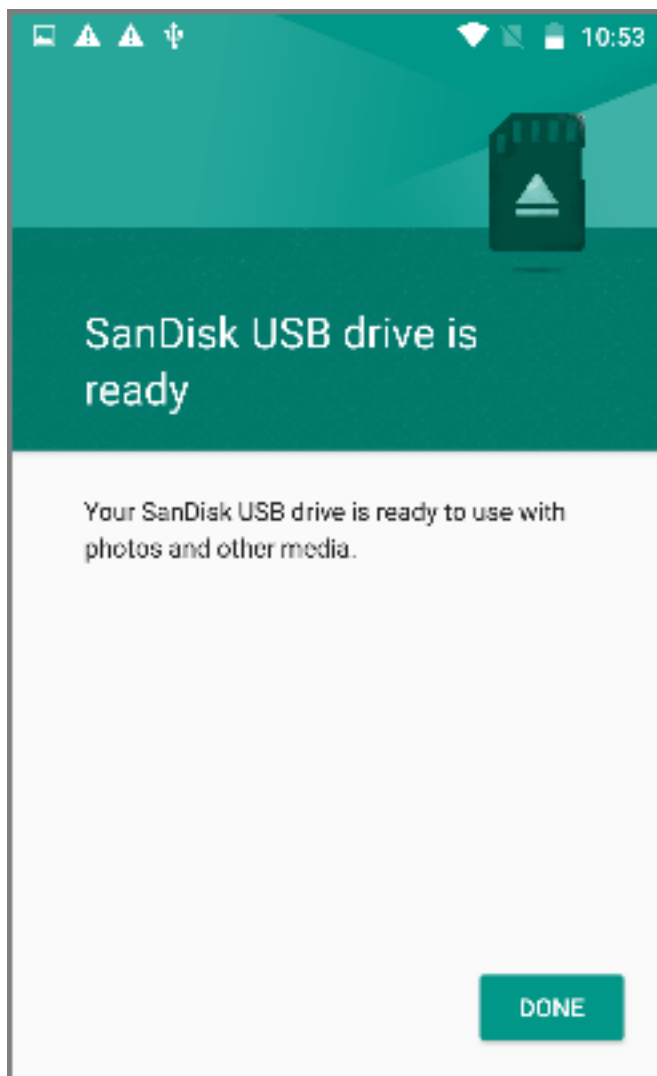


2. Select the **Corrupted USB drive** notification. The following screen appears.



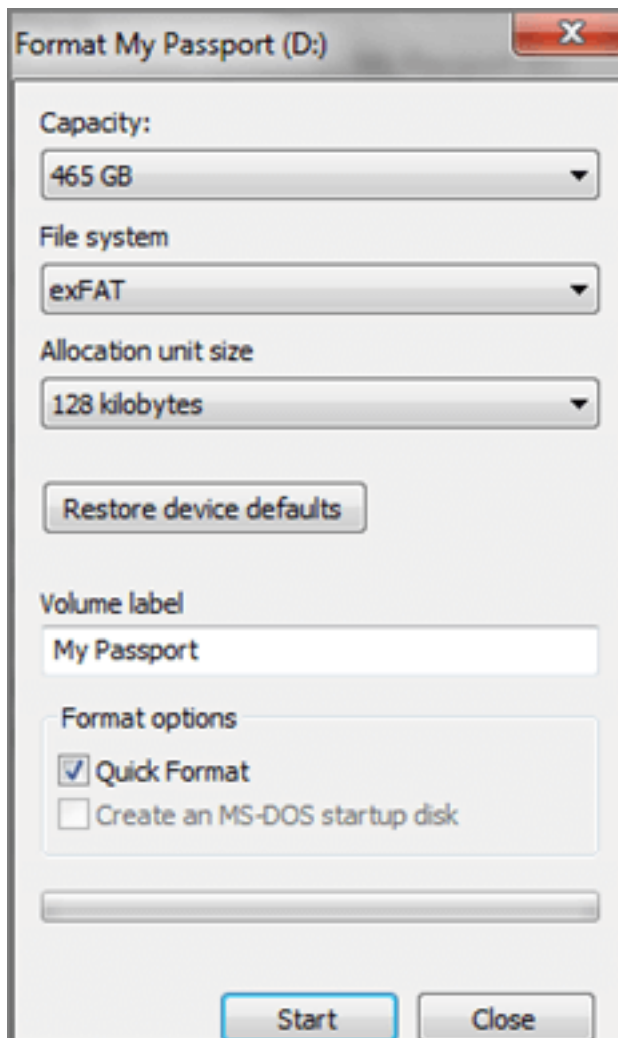


3. Follow the instructions to erase and format the device. Upon completion, the following screen appears.



### To format the storage device from the PC:

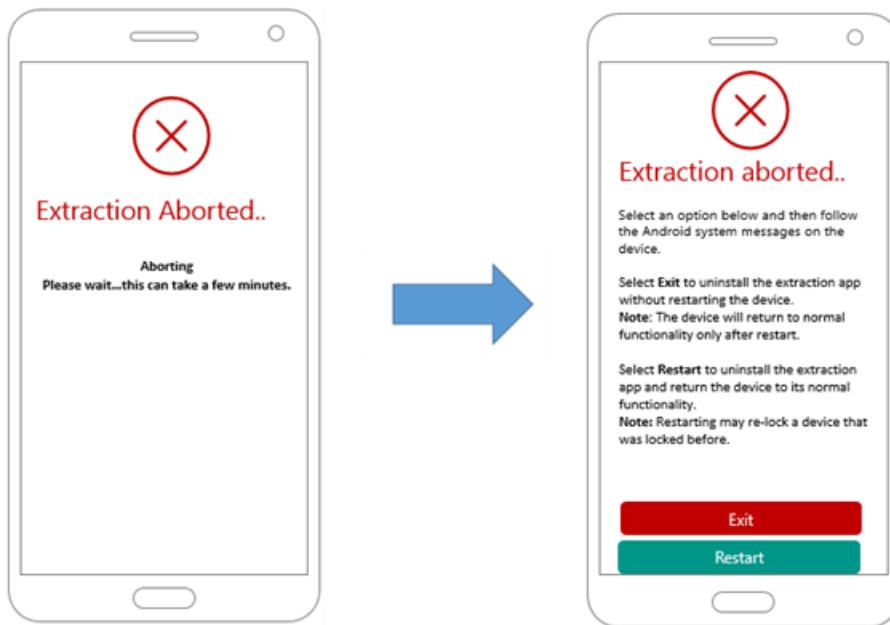
1. Plug the hard drive into your Windows PC. Right-click on the D drive and select “Format”  
The following window appears.



2. Under File System, select exFAT.
3. Click **Start** and complete the format process.

### 6.3.2.1.1. Extraction aborted

If **Abort** was selected during the extraction process, the screen on the left will appear. After some time (up to a few minutes) the screen on the right will appear.



- » Select **Exit** to uninstall the extraction app without restarting the device.



The device will only return to normal functionality after restart.

- » Select **Restart** to uninstall the extraction app and return the device to its normal functionality.



Restarting may re-lock a device that was locked before.

### 6.3.2.1.2. Extraction failed

If the extraction failed for any reason, the following screen appears with the failure reason.



- » Select **Exit** to uninstall the extraction app without restarting the device.



The device will only return to normal functionality after restart.

- » Select **Restart** to uninstall the extraction app and return the device to its normal functionality.



Restarting may re-lock a device that was locked before.

## 6.4. Boot loader (FW flashing)

The Boot loader (FW flashing) extraction method uses boot loader reflashing, which enables a physical extraction while bypassing user lock (non-secure startup). This method is for Qualcomm-based Samsung Galaxy S7 devices running firmware version of Android 7.x. For a complete list of supported devices, refer to UFED Supported Devices document in [MyCellebrite](#). This extraction does not support extractions from a memory card.

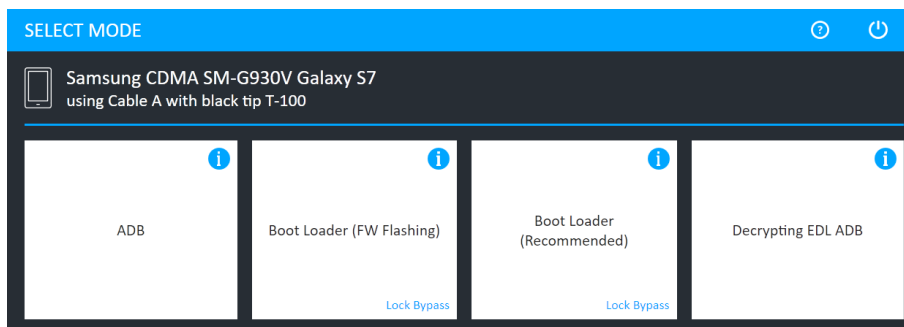


This Boot loader (FW flashing) extraction method requires the device's firmware to be flashed. In some cases the device may experience unexpected behavior and you will need to flash the original device firmware, which causes a device wipe. Before using this method, we recommend trying other Physical bootloader methods.

### To perform Boot loader (FW flashing):

1. Click **Mobile device** and identify the device, then click **Physical**.

The Select Mode screen appears:



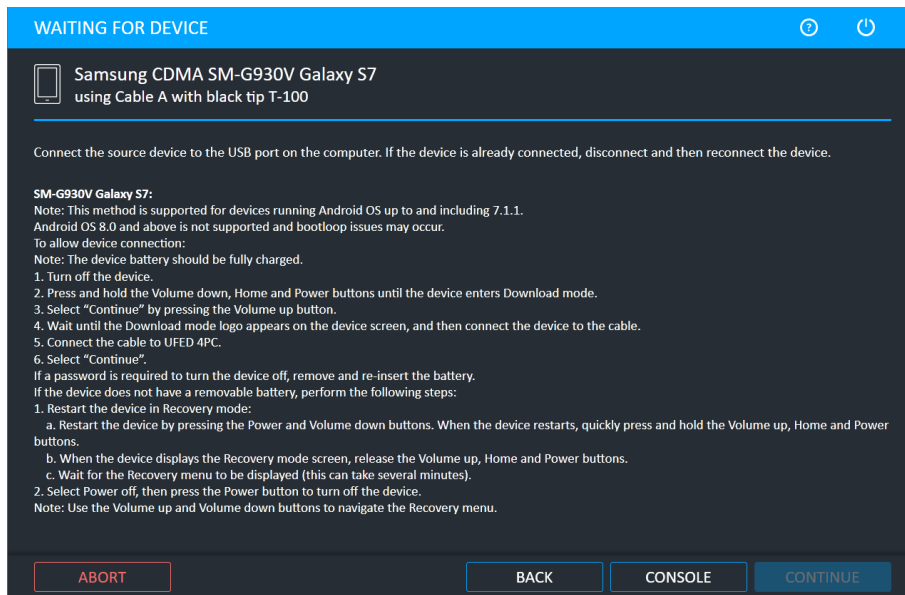
2. Select **Boot loader (FW Flashing)**.



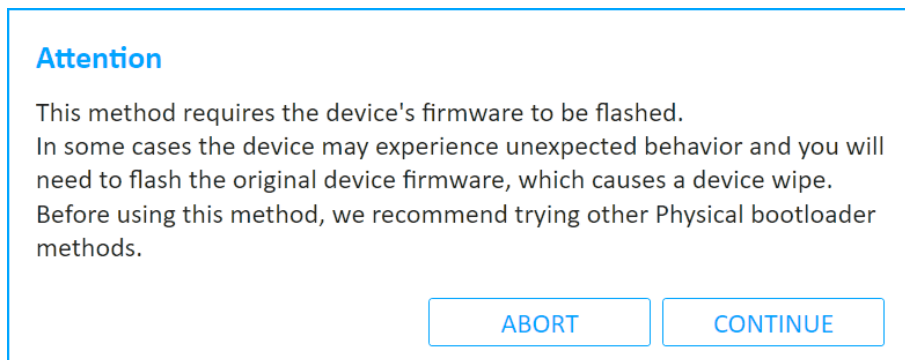
For information on using optional timeframe and party filters, refer to the *Overview Guide*.

The following Select extraction location window appears.

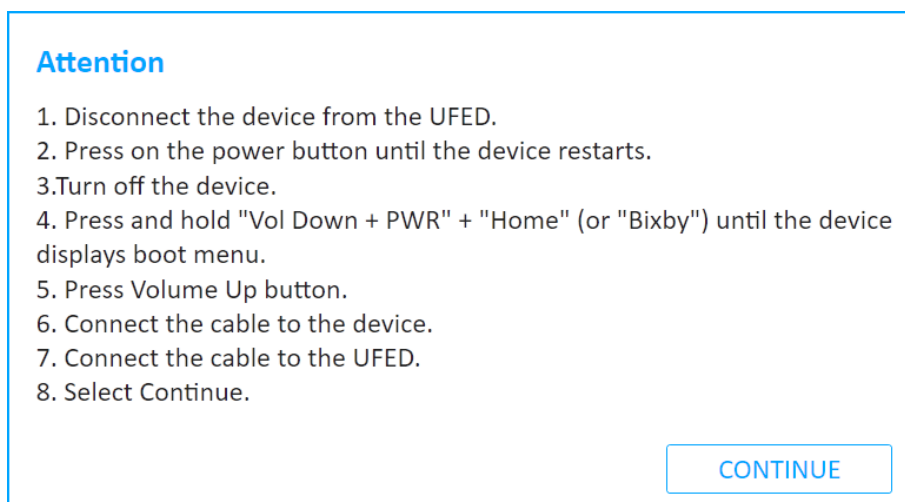
3. Select the extraction location. The Waiting for Device screen appears.



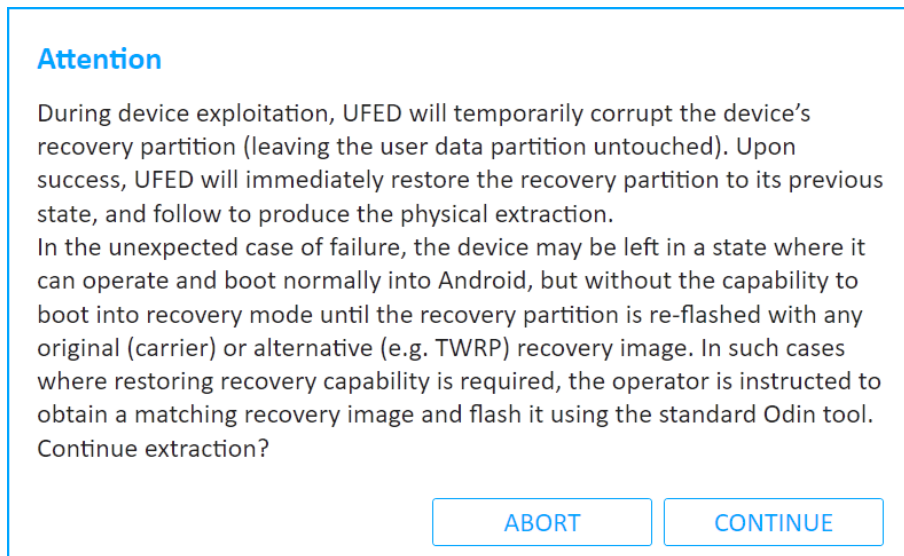
4. Follow the on-screen instructions to place the device in Download mode, then connect the required cable to the device and UFED.
5. Click **Continue**. The following window appears.



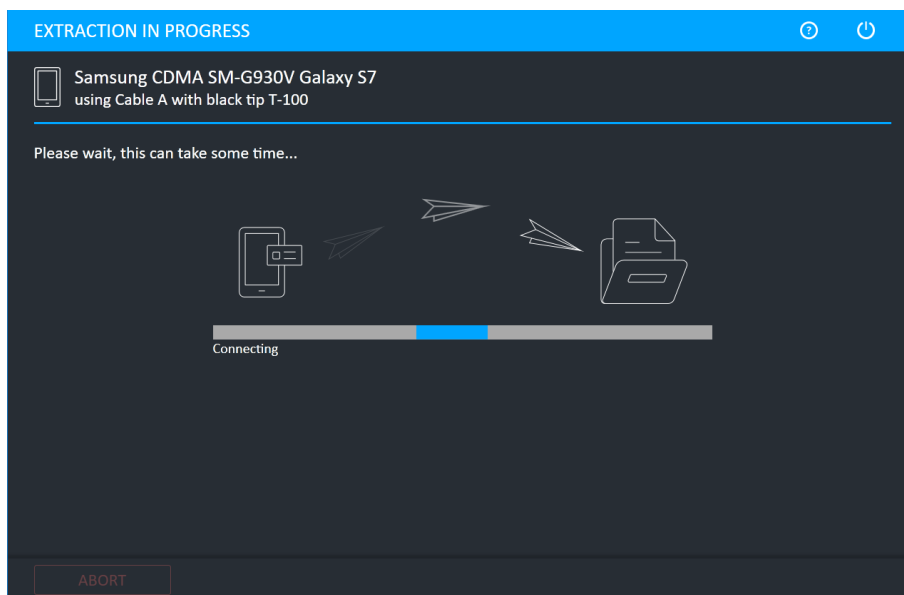
6. Click **Continue** to flash the device's firmware. The following window appears.



7. Follow the on-screen instructions to place the device in Download mode again, then connect the required cable to the device and UFED.
8. Click **Continue**. The following window appears.



9. Click **Continue**. The Extraction in Progress window appears.



10. Follow any on-screen instructions.



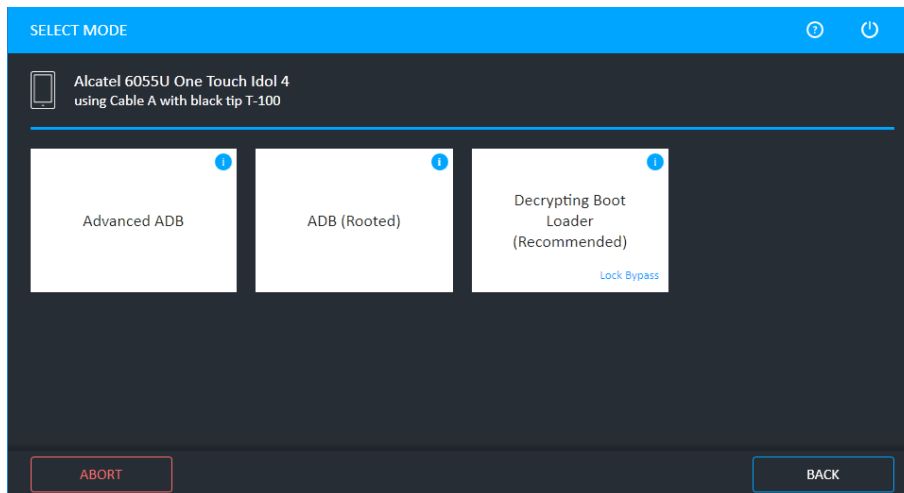
## 6.5. Decrypting boot loader

This extraction method performs a physical extraction on encrypted Android devices with the following Qualcomm chipsets: 8909, 8916, 8939, 8952, and 8396. It performs the extraction when the device is in boot loader mode. It bypasses the user lock and is forensically sound.

### To perform a Decrypting boot loader extraction:

1. Click **Mobile device** and identify the device, then click **Physical**.

The Select Mode window appears:



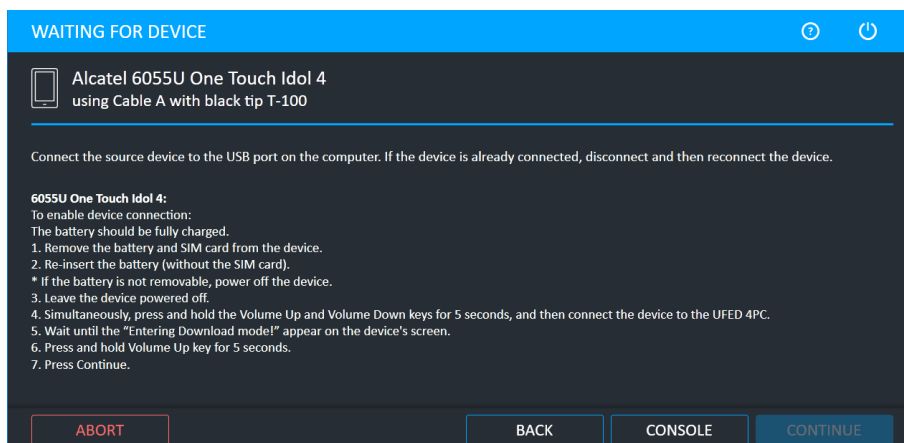
2. Click **Decrypting Boot Loader**.



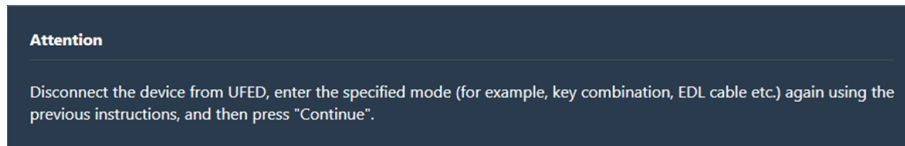
For information on using optional timeframe and party filters, refer to the *Overview Guide*.

The Select Extraction Location window appears.

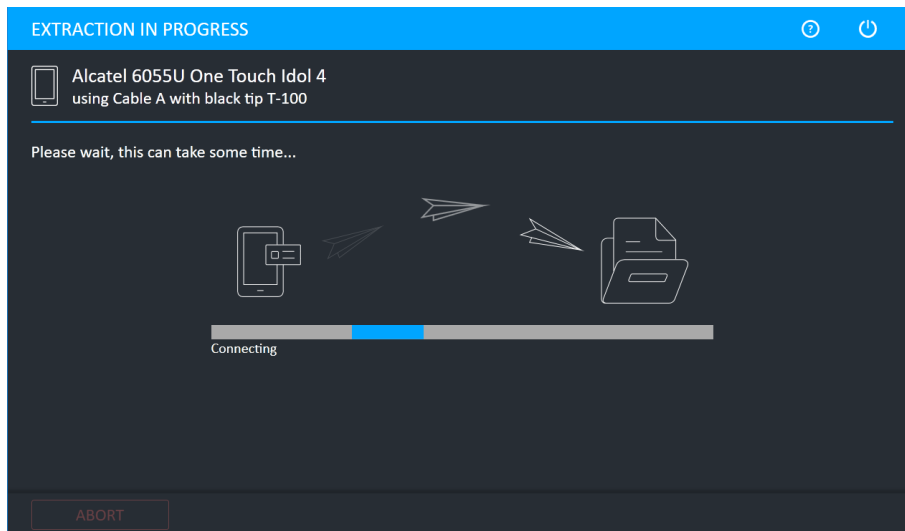
3. Select the extraction location. The Waiting for Device window appears.



4. Follow the on-screen instructions to place the device in the required mode. Click **Continue** when enabled.



5. Disconnect the device from UFED, enter the specified mode again (for example, key combination, EDL cable etc.) using the previous instructions, and then click **Continue**. The following window appears.



## 6.6. Forensic recovery partition

An extraction method that performs a physical extraction while the device is in recovery mode. UFED replaces the device's original recovery partition with Cellebrite's custom forensic recovery partition. The original recovery partition on the Android device can be considered as an alternative boot partition that may also change the user data, while Cellebrite's recovery partition does not affect any of the user data. This extraction method bypasses the user lock from a number of Samsung Android devices and is forensically sound. It does not support extractions from a memory or SIM card.

For a complete list of supported devices, refer to the UFED Phone Detective Mobile App or the UFED Supported Devices document in [MyCellebrite](#).



It is recommended to use the Forensic recovery partition method when other physical extraction msm-methods (e.g., Bootloader) are not successful, or not available (e.g., if the Android firmware version is not supported).

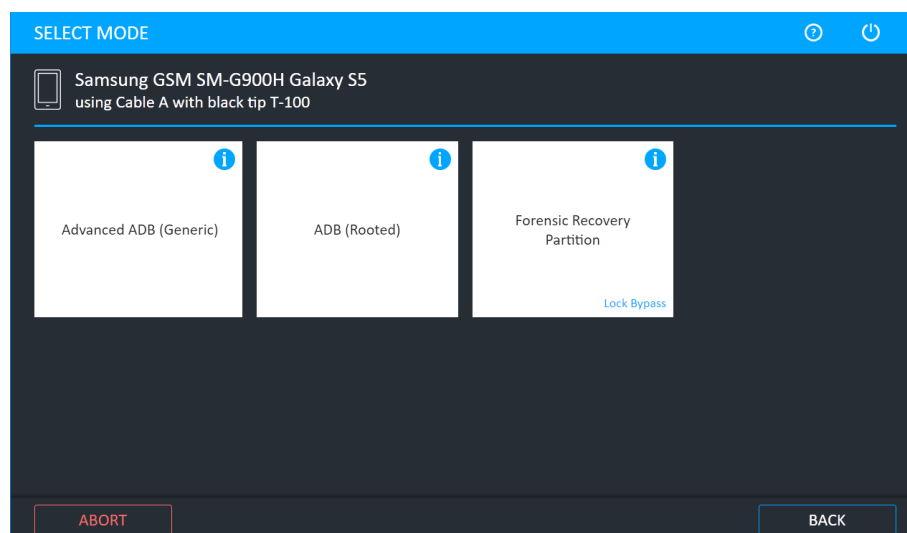


If the device does not start correctly after using this extraction method, use the Exit Android Recovery Mode device tool. See [Exit Android recovery mode \(on page 127\)](#).

### To perform a forensic recovery partition extraction:

1. Click **Mobile device** and identify the device, then click **Physical**.

The Select Mode screen appears:



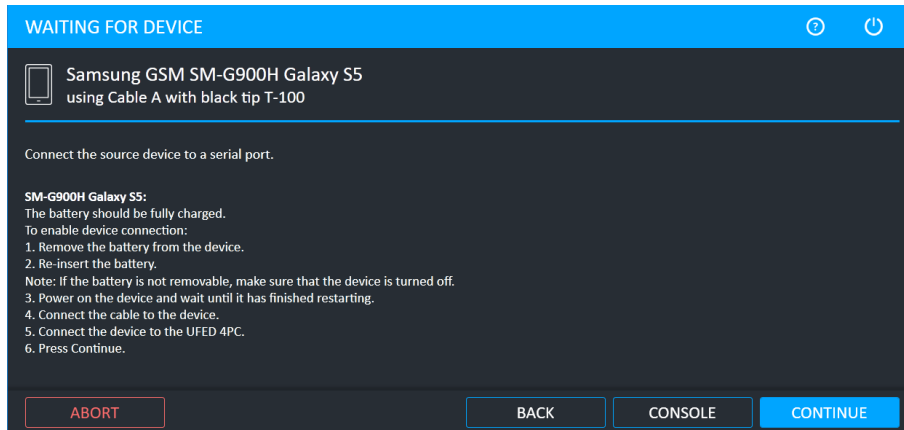
2. Select **Forensic Recovery Partition**.



For information on using optional timeframe and party filters, refer to the *Overview Guide*.

The following screen appears.

The Waiting for Device screen appears.



3. Click **Continue**. The following warning is displayed.

**Attention**

This method replaces the recovery partition on the device in order to extract user data.

For the recovery partition to function correctly, do not disconnect the device until the extraction completes.

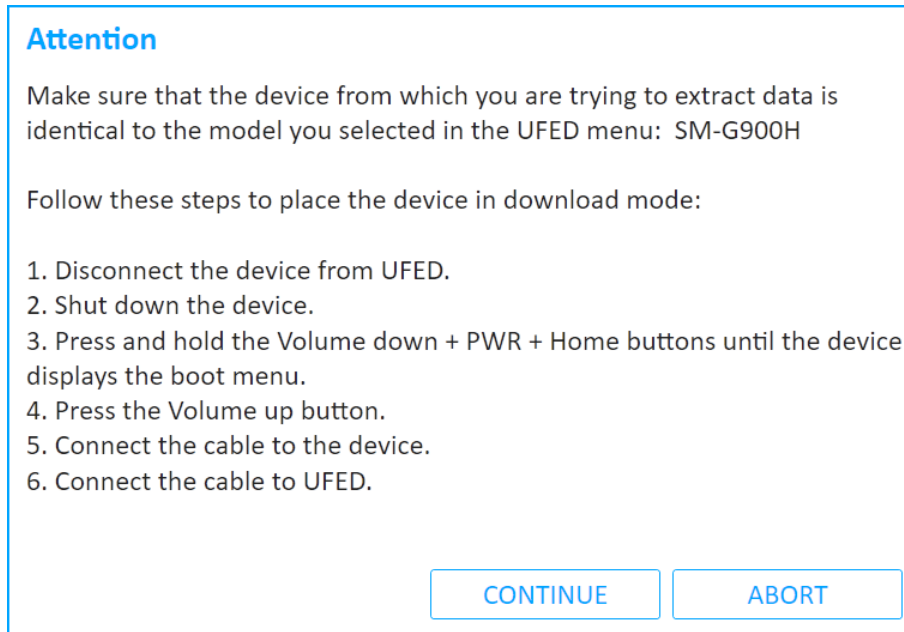
Warning: This method activates the Samsung KNOX warranty bit on the device.

This permanently voids the warranty and prevents further access to data stored in KNOX containers.

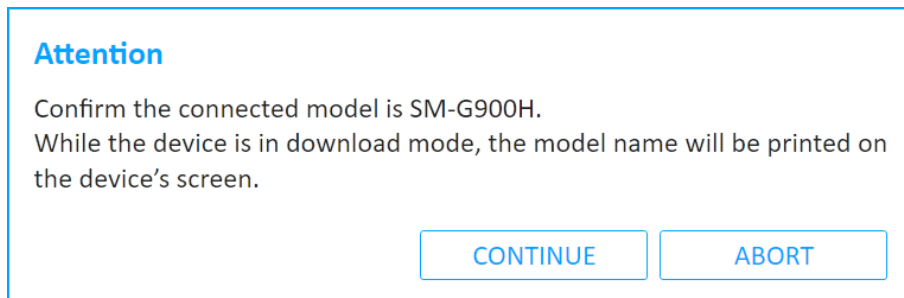
CONTINUE

ABORT

4. Click **Continue**. The device will be placed in download mode. The following screen appears.

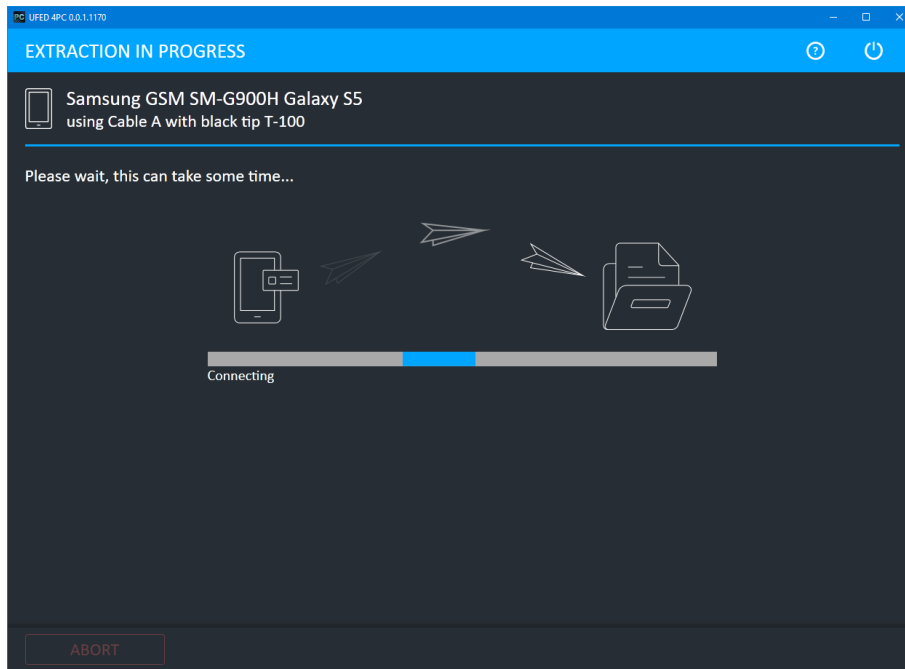


5. Click **Continue**. The following screen appears.



6. Click **Continue**. The following screen appears.
7. Follow the instructions to place the device in Download mode. Force it to restart by pressing the Power and Volume down buttons. When the device restarts, quickly press the Volume up, Home and Power buttons. Click **Continue** when **Downloading** appears on the device's screen (this can take a few minutes).

The Extraction in Progress screen appears.



8. Follow any on-screen instructions.

## 6.7. Smart ADB

The Smart ADB extraction method enables you to perform physical extractions on Android devices that include the "November 2016" security patch. This method is supported by OTG compatible devices, with OS versions 6.0 and above. Only security unlocked devices are supported.



On some devices, you may need to enable the OTG option.



It is recommended to place the device in Flight mode.

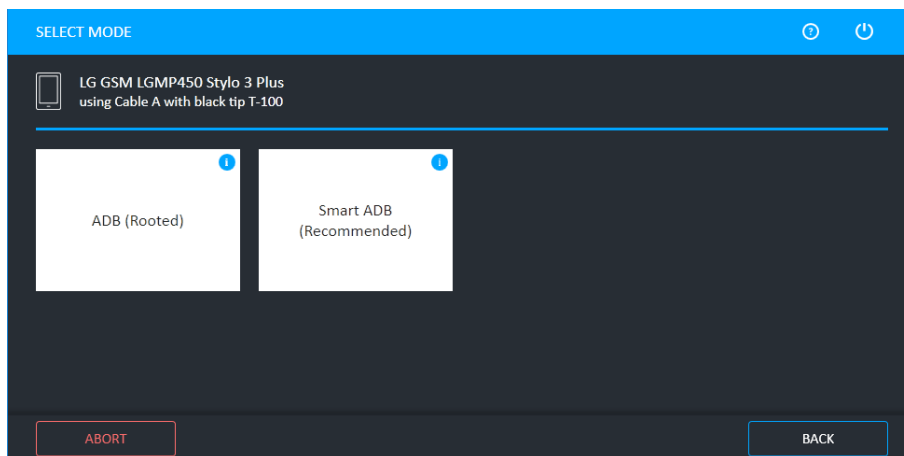


If a specific device is not supported, we recommend that you use a similar model or any generic Advanced ADB profile.

### To perform a Smart ADB extraction:

1. Click **Mobile device** and identify the device, then click **Physical**.

The Select Mode screen appears:

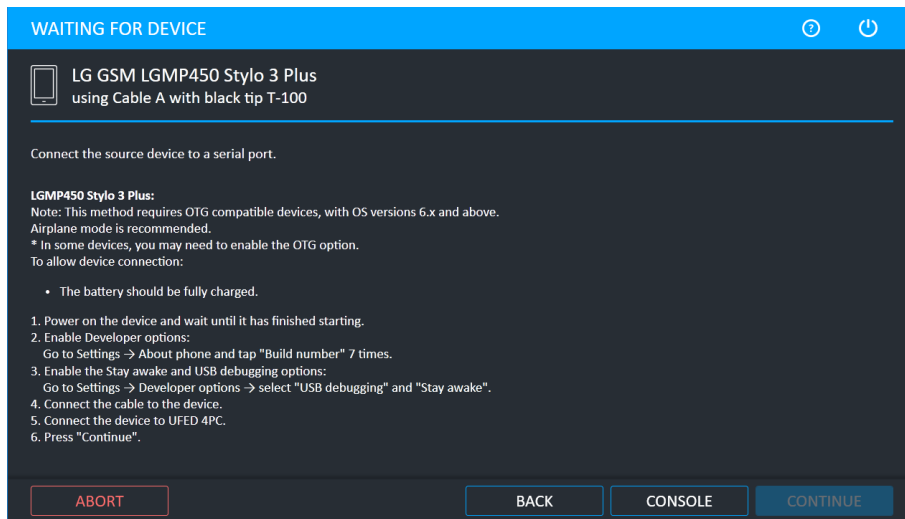


2. Click **Smart ADB**.

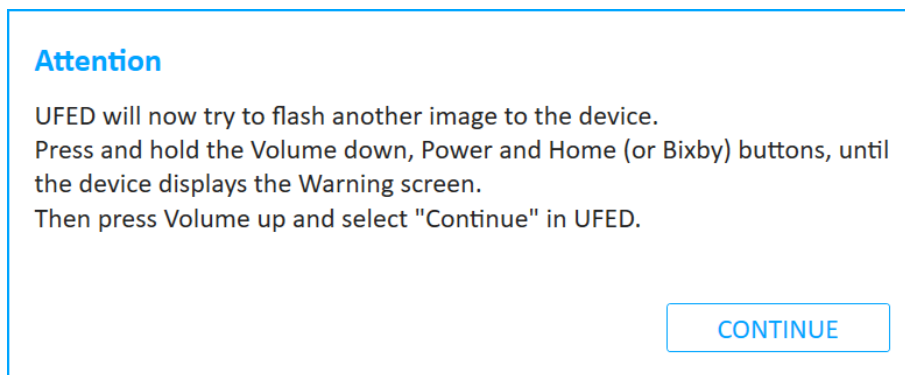


For information on using optional timeframe and party filters, refer to the *Overview Guide*.

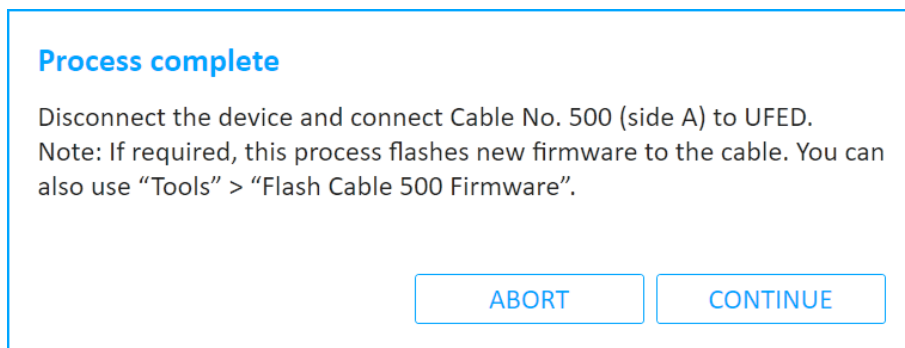
The Waiting for Device screen appears.



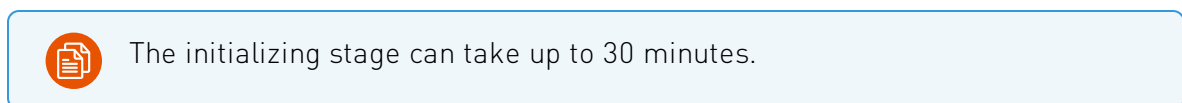
3. Follow the on-screen instructions then click **Continue**. The following window appears.



4. Click **Continue**. The following window appears.



5. Disconnect the device and connect Cable No. 500 (side A) to UFED, then click **Continue**.







If required, this process flashes new firmware to the cable. You can also use the [Flash Cable 500 Firmware \(on page 127\)](#) tool.

The following window appears.

### Process complete

Connect Cable No. 501 to the device and the other end of the cable to Cable No. 500.

CONTINUE

6. Connect Cable No. 501 (or other specified cable) to the device and the other end of the cable to Cable No. 500, then click **Continue**. The initialization process starts.

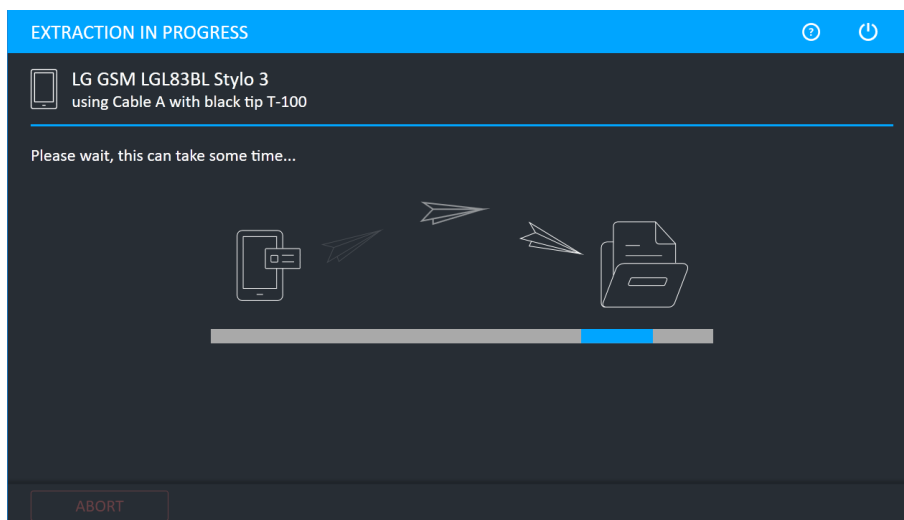
The following window appears.

### Attention

Disconnect the cables, and connect the device to UFED with Cable No. 100.

CONTINUE

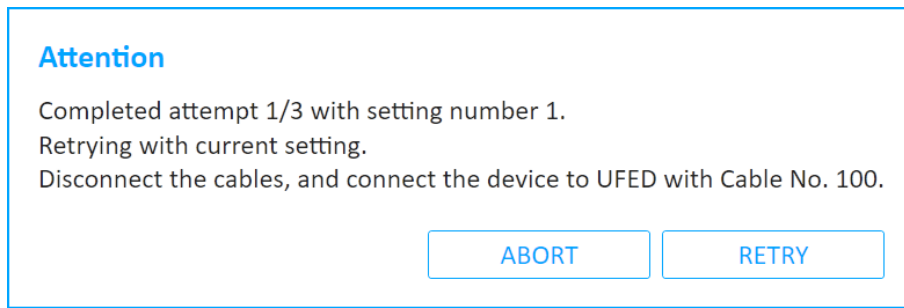
7. Disconnect Cable No. 500 and reconnect the device using Cable No. 100 (or other specified cable). Click **Continue** to start the extraction. The following window appears.



When the extraction completes, the Extraction completed successfully window appears. If Cellebrite UFED/Responder could not find a setting for the specific device, UFED can

attempt other potential settings. This process requires user interaction and takes time to complete.

8. Click **Continue** to try the extraction with other settings. The following window appears.



9. Disconnect the cables and connect the device to UFED with Cable No. 100 (or specified cable), then click **Retry**.

## 7. Capture images and screenshots

The Cellebrite UFED camera enables you to collect evidence by taking pictures or videos of a device (see [Capturing images \(on the next page\)](#)). You can also use a Screenshot feature to capture internal screenshots directly from a Blackberry, Android or iOS device (see [Capturing screenshots \(on page 100\)](#)). Both these options can be useful as complimentary evidence or in instances when data cannot be extracted from a device. You can add notes, categories and bookmarks to the pictures and videos, which will be visible in Physical/Logical Analyzer.

The collected evidence can be shown within a standalone custom report or in addition to the extracted information. The report includes information about the device, connection type, Cellebrite UFED version, and serial number. Image information includes file name link, file size, date and time, MD5 and SHA256 hash information. The images are located in a folder called Snapshots and are in PNG format. Video information includes file name, file size, date and time, and a link to the file. The videos are located in a folder called Videos and are in AVI format.

### 7.1. The Cellebrite UFED camera

The Cellebrite UFED camera is offered as an add-on and it is controlled by the Cellebrite UFED/Responder. All necessary drivers are preinstalled with the application. The Cellebrite UFED camera includes a camera stand, which enables you to adjust the height and the angle of the Cellebrite UFED camera, a pad to place the device, and an anti-glare pad to prevent glare when taking pictures. Connect the camera to an available USB port of the computer.

## 7.2. Capturing images

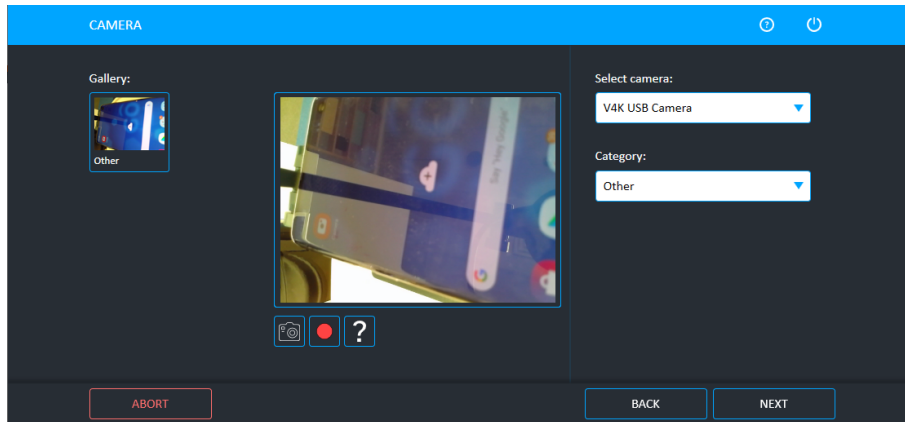
You can take pictures or videos of a device.

### To capture images or videos:

1. Click **Camera**.



The Select Extraction Location screen appears.






2. Connect the Cellebrite UFED camera to a USB port on the computer. The following window appears.



If you have multiple cameras, you can choose the required camera in Select camera box.

3. Do one of the following:

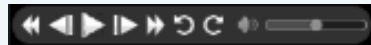
» Click  to start a video recording and click  to stop the video recording.

- » Click  to take a picture.
- » Click **Other** to change the default category. Images and videos will be displayed in Physical/Logical under these categories.
- » Click an image or video, to add notes, bookmarks () , categories () , or delete the file (). Click  to move back to live view.



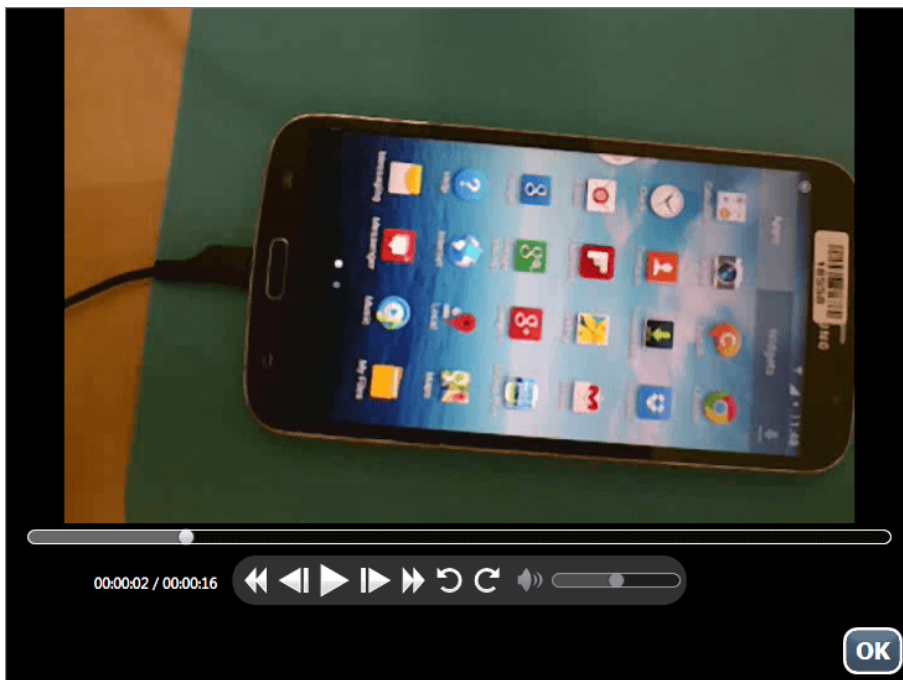
To rotate a picture or video, or play a recorded video, click the picture or video, and then click the picture or video in the leftmost

screen. Use the rotate buttons  or video buttons



. See the following examples.





4. Click **Next** to continue.

## 7.3. Capturing screenshots

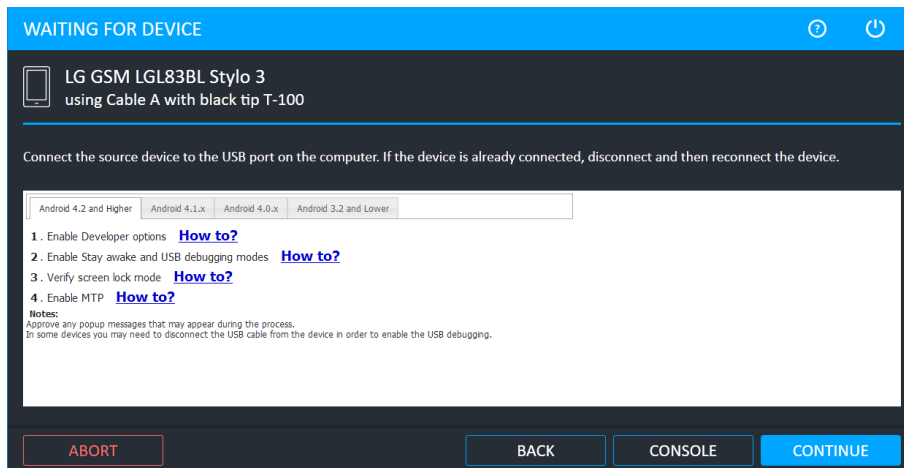
The Screenshot feature captures internal screenshots directly from a Blackberry, Android or iOS device.

### To capture screenshots from the devices:

1. Click **Mobile device** and identify the device, then click **Screenshots**.

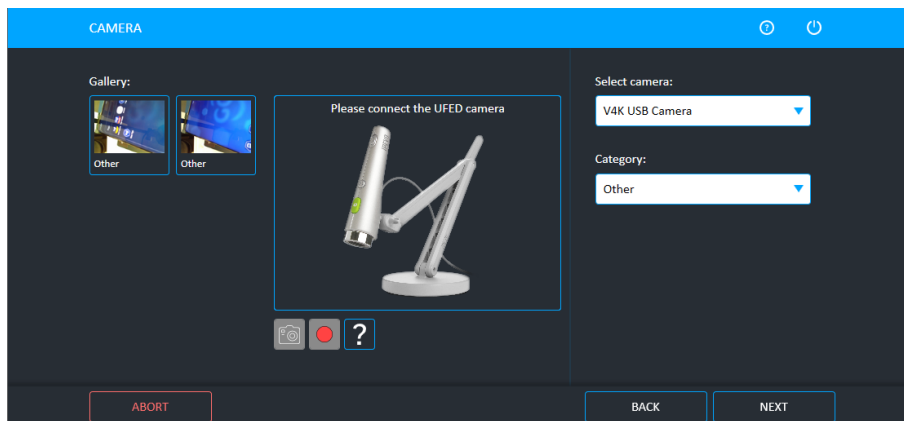
The Select Extraction Location screen appears.

The Waiting for Device screen appears.



2. Follow the instructions to connect the device.
3. Click **Continue**.

The Screenshots screen appears.



If you have multiple cameras, you can choose the required camera in Select camera box.



4. Capture the desired screenshots and click **Next**. The Capture Screenshots Summary screen appears.

## 8. Chat capture

Chat Capture is an automated screen capturing process that allows users to extract and analyze selective chat conversations from third party application data.

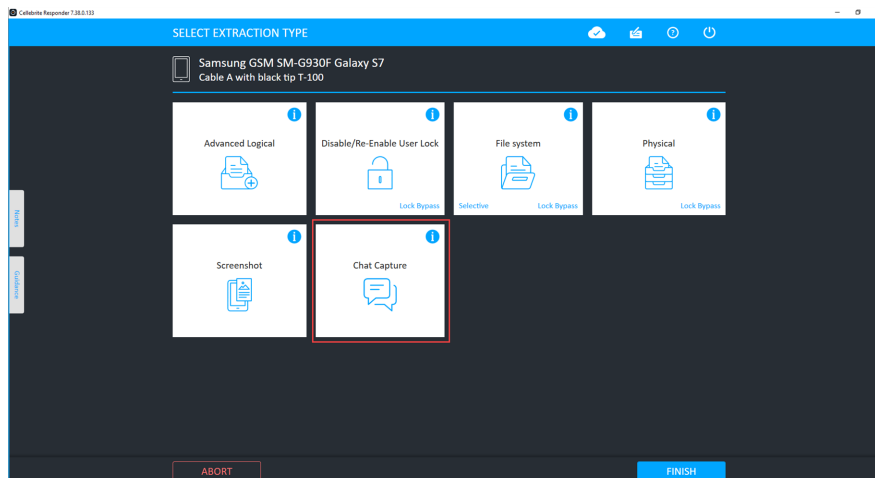
There are two modes available:

- » **By application** – Automatically capture data from supported apps like WhatsApp based on conversation name and date range. Users can also perform text search on the captured screens.
- » **Generic** – Semi-automated mode to capture any scrollable area on the device screen.

### 8.1. Performing a Chat capture by application

In addition to capturing the chat, this mode will also capture chat information such as chat name and participant details.

1. Click **Mobile device** and identify the device, then click **Chat capture**.

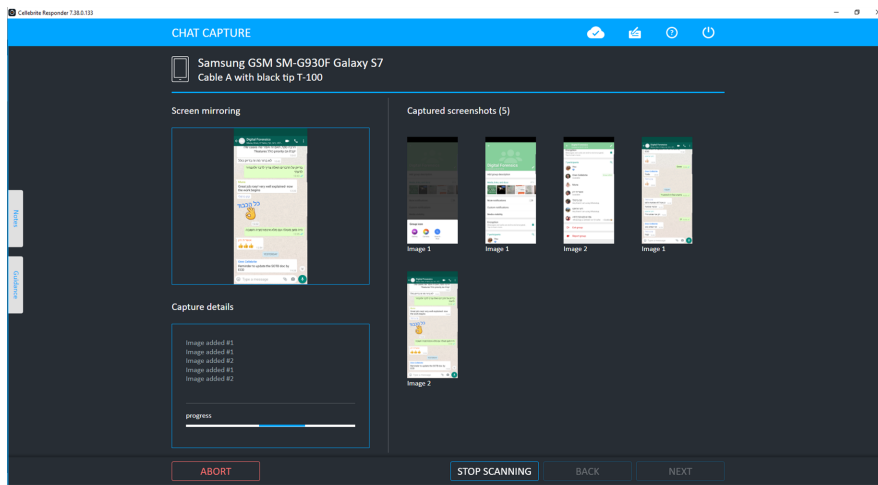


2. Select the application from which to capture a chat.
3. Select a predefined timeframe or create a custom timeframe.
4. Click **Next**.

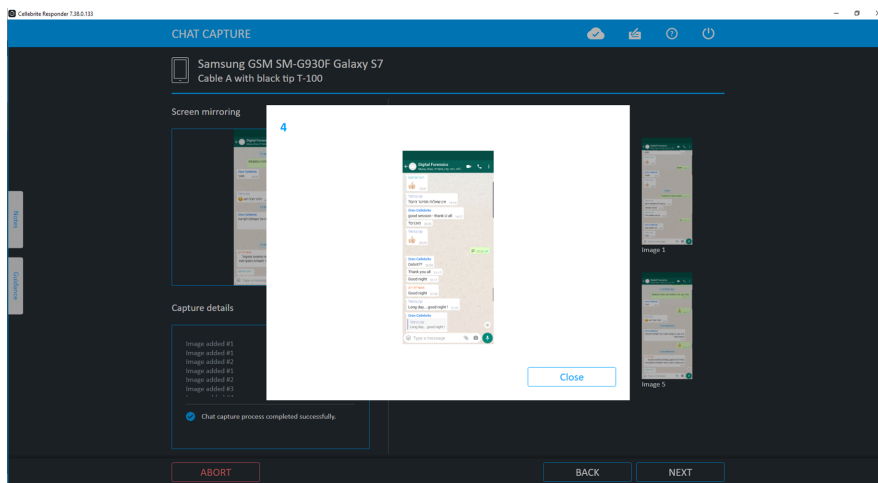


When using Chat capture, you are entering a live conversation. Once a chat is entered, unread messages will be marked as read.





8. To view a single screenshot, click on it to enlarge.



9. Click **Next** when finished.

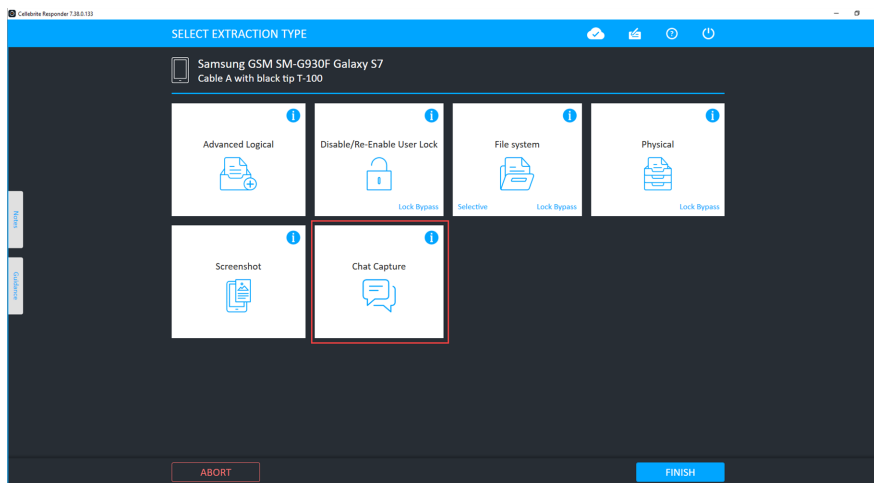


Captured screenshots can be viewed and analyzed in Physical/Logical Analyzer under the Chats model.

## 8.2. Performing a Chat capture in Generic mode

In addition to capturing chats, Generic mode can be useful to capture any element of data such as social media feeds, forums, etc.

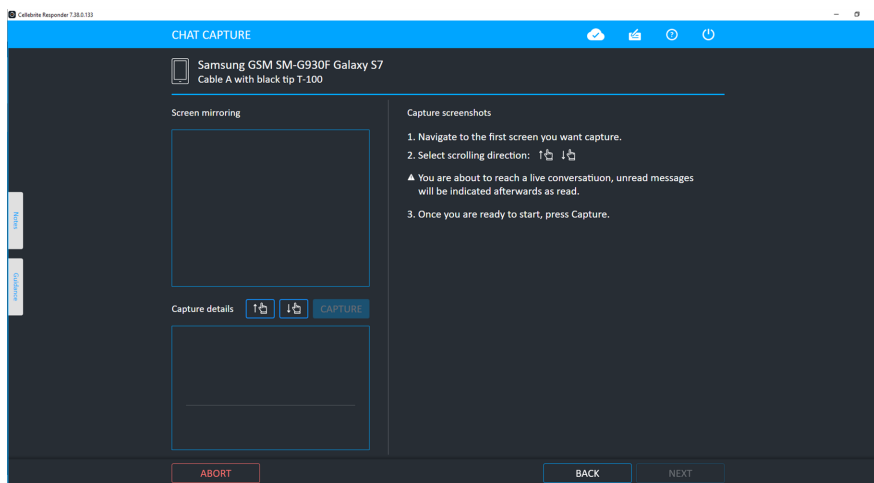
1. Click **Mobile device** and identify the device, then click **Chat capture**.



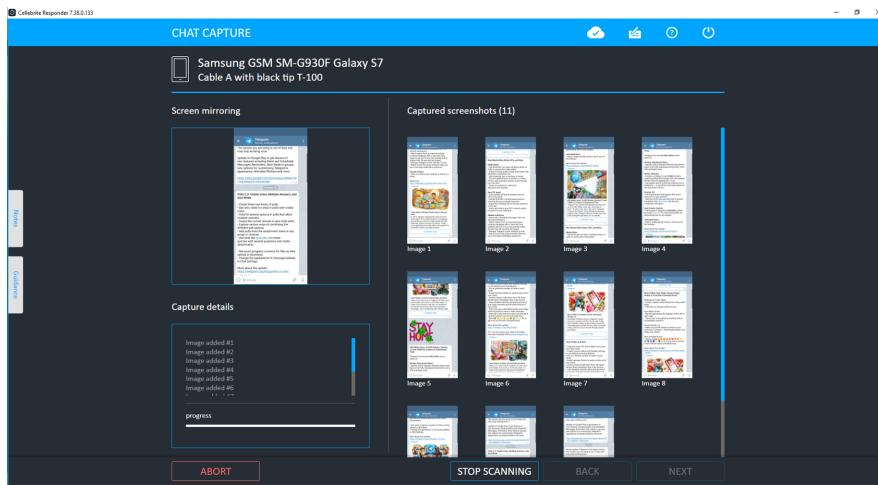
2. Select **Generic**.
3. Click **Next**.
4. Navigate to the relevant app and then to the first screen that you want to capture.



5. Select scrolling direction .
6. When ready, click **Capture**.



7. The chat will be automatically captured. The captured screens appear under **Captured screenshots**.



8. To view a single screenshot, click on it to enlarge.
9. Click **Next** when finished.



Captured screenshots in Generic mode can be viewed and analyzed in Physical/Logical Analyzer or Responder viewer under the Images model.

You will be able to perform a text search of the captured screens but only in chat applications that support the search functionality. \*Available in Physical/Logical Analyzer only.

## 9. SIM card functionality

The **SIM Card** functions enable you to perform various SIM card related functions:

- » Sim data extraction
- » Clone SIM
- » File system extraction

### 9.1. SIM data extraction

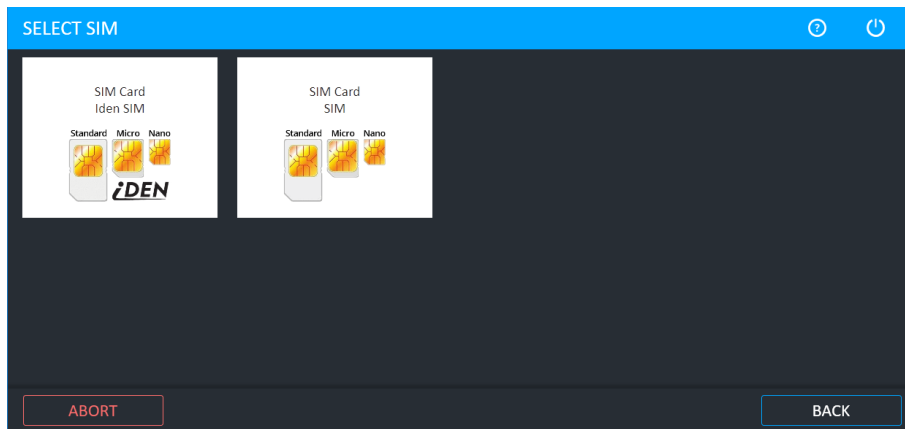
The SIM Data Extraction function enables you to perform logical extraction from a SIM or USIM card.

#### 9.1.1. Performing SIM data extraction

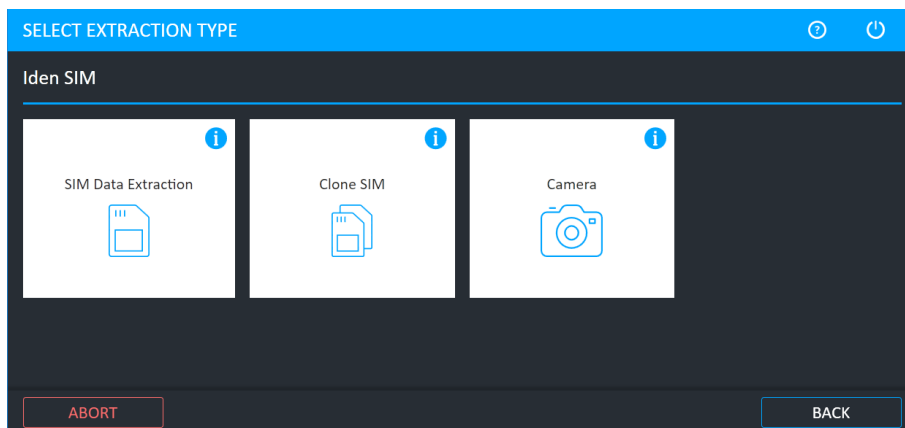
The following example is performed using a SIM Card.

**To perform the SIM Data Extraction:**

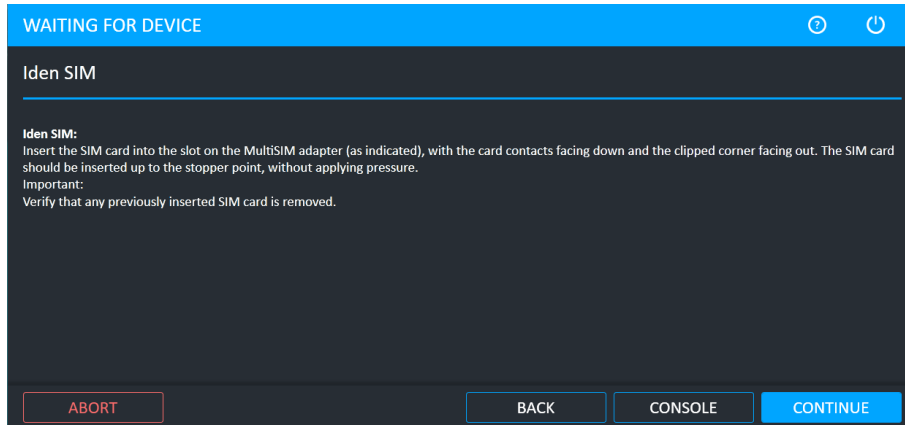
1. Click **SIM Card**. The following window appears.



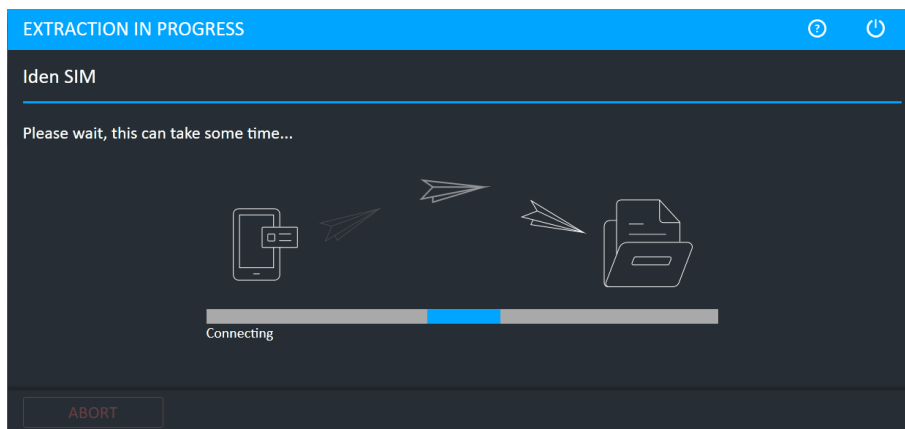
2. Click either **SIM** or **Iden SIM**. The Select Extraction Type window appears.



3. Click **SIM Data Extraction**. The Select Extraction Location window appears.  
The Waiting for Device screen appears.



4. Insert the SIM card into the SIM card slot.
5. Click **Continue**. The extraction begins.



The following window appears.



## Authenticating

Use PIN (3  
attempts left)

Use PUK (10  
attempts left)

Skip protected  
data

CANCEL

6. Click **Use PIN**, **Use PUK** or tap **Skip protected data**.

#### 9.1.1.1. The extracted SIM data folder

At the end of the SIM data extraction process, the extracted SIM data is saved in the location you selected previously.



The extracted SIM data folder is named "UFED SIM card" with the extraction date and counter: "UFED SIM card SIM card <DATE> {001}"

If you selected to extract to the local drive, the extracted SIM data folder is located inside the application's Backup folder.

The extracted SIM data folder contains a forensic report of extracted data in both HTML and XML formats and call log file (\*.clog).

## 9.2. Clone SIM

The Clone SIM ID function enables you to copy the SIM ID from one SIM card to a UFED SIM ID Access Card.

Cloning the SIM ID provides a suitable solution to several problems facing forensic examiners, by allowing extraction of the device data:

- » While preventing the cellular device from connecting to the network, rendering the device invisible to the network without the ability to send or receive calls or SMS messages, and thereby preserving the device's current information. (No Faraday Bag is required to block RF signals).
- » When the original SIM is not available, by manually programming the ICCID or IMSI into the Cloned SIM ID Card to mimic the original missing card.
- » When the SIM card is PIN locked, by cloning the identification of the original SIM, which allows extraction of the device data without losing critical data including call history and SMS messages.

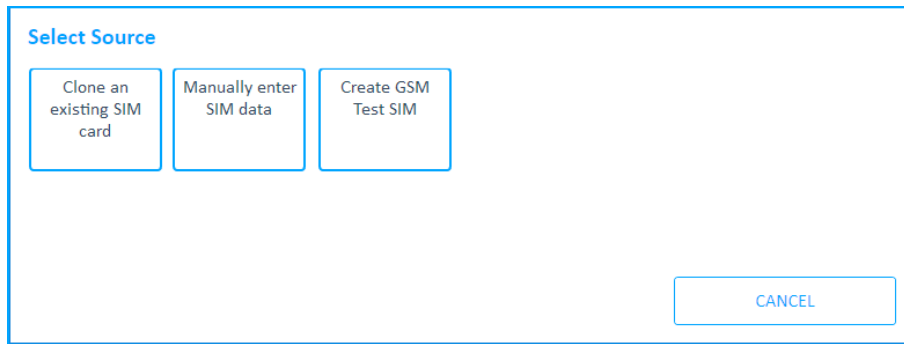
There are three different ways that a SIM card can be cloned:

- » Clone an existing SIM card - to create a cloned SIM to use to extract device data without a network connection. See [Cloning an existing SIM card ID \(below\)](#).
- » Manually enter SIM data - to manually program the ICCID and IMSI to the cloned SIM card. See [Entering SIM data manually \(on page 114\)](#).
- » Create GSM Test SIM - The GSM test SIM card is used to extract device data when the original SIM is not available – a default ICCID and IMSI are programmed into the Cloned SIM ID Card to mimic the original missing card. See [Creating a GSM test SIM \(on page 118\)](#).

### 9.2.1. Cloning an existing SIM card ID

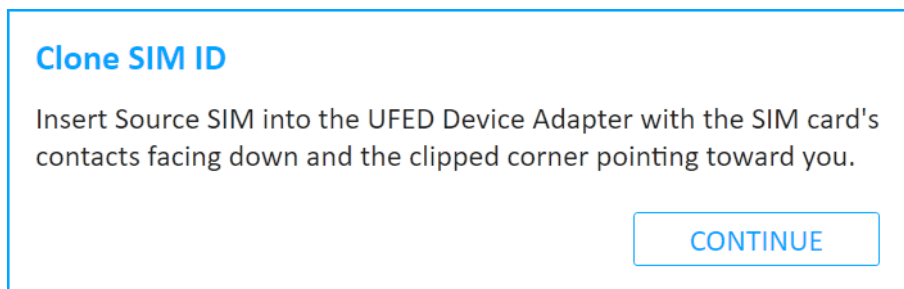
## To select the source and clone the SIM card:

The **Select Source** screen appears.

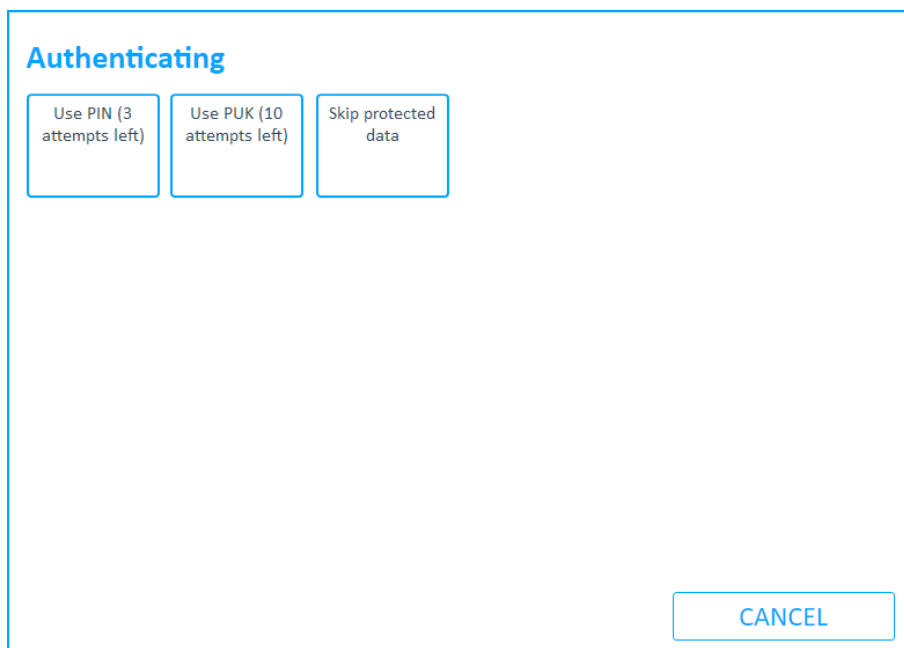


4. Click **Clone an existing SIM card**.

The Clone SIM ID prompt appears.

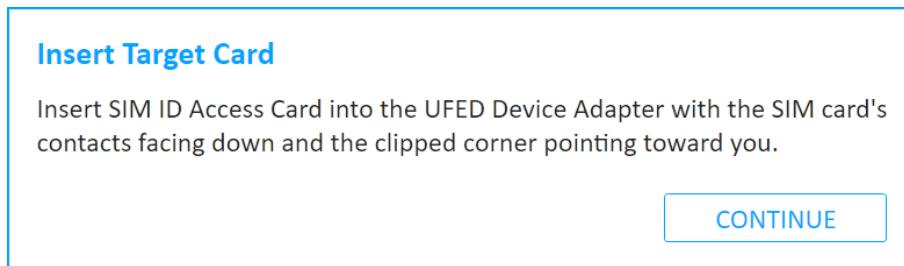


5. Check that the right SIM was inserted into the SIM card reader slot.
6. Click **Continue**. The following window appears.



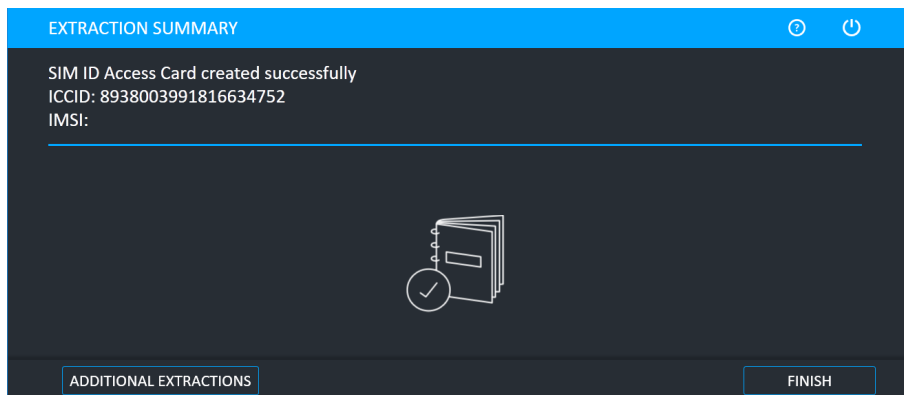
7. Click **Use PIN**, **Use PUK** or tap **Skip protected data**. The Extraction in Progress Source screen appears.

When the information has been extracted from the SIM, the Insert Target Card prompt appears.



8. Remove the original SIM card from the SIM card reader.
9. Insert a UFED SIM ID Access Card into the SIM slot.
10. Click **Continue**.

At the end of the data process, a summary of the SIM cloning process is displayed, detailing the ICCID and IMSI information of the cloned SIM card.



11. To end the process and return to the home screen, click **Finish**.

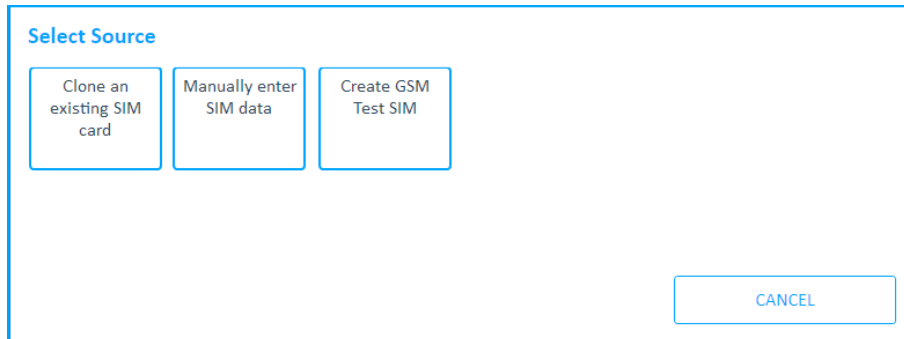
### 9.2.2. Entering SIM data manually

1. In the home screen, click **Clone SIM**.

The Waiting for Device screen appears.

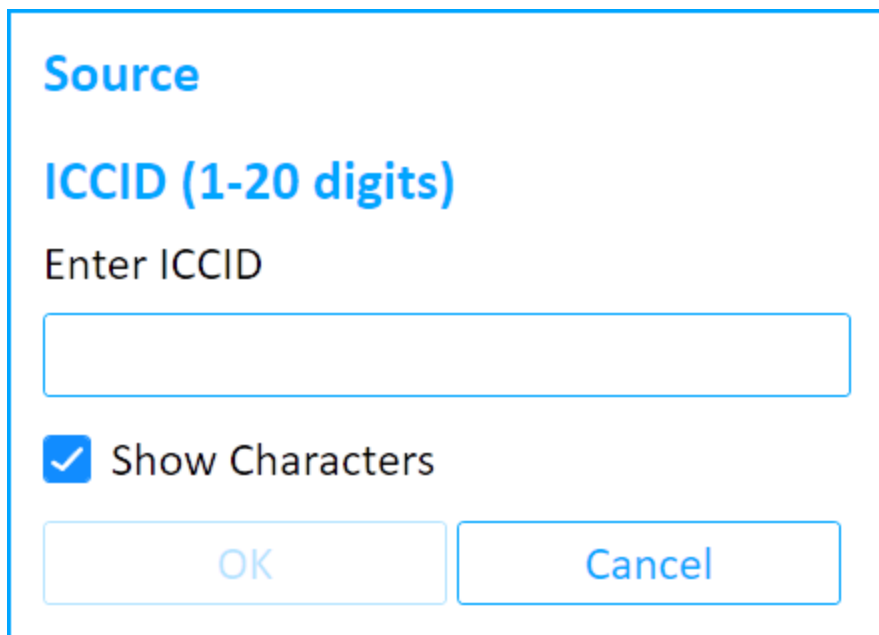
2. Insert the UFED SIM ID Access card.
3. Click **Continue**.

The Select Source screen appears.



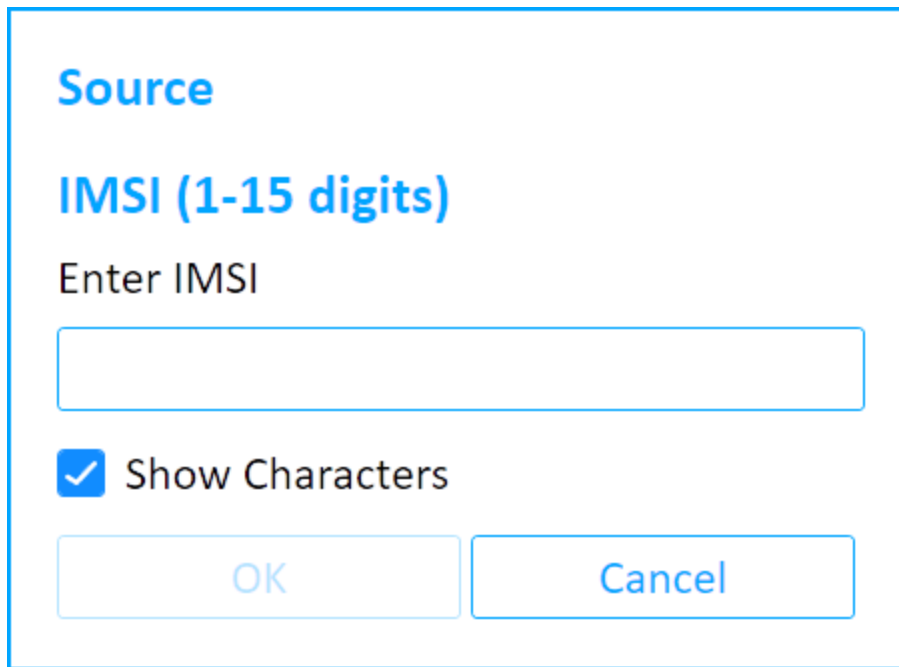
The 'Select Source' screen features a title bar at the top left. Below it, three rectangular buttons are arranged horizontally: 'Clone an existing SIM card', 'Manually enter SIM data', and 'Create GSM Test SIM'. A 'CANCEL' button is positioned in the bottom right corner of the screen.

4. Click **Manually enter SIM data**. The following screen appears.



The 'Source' screen has a title bar at the top. Below the title, the text 'ICCID (1-20 digits)' is displayed in a large, bold font. Underneath, the instruction 'Enter ICCID' is followed by a single-line text input field. A checkbox labeled 'Show Characters' is checked. At the bottom, there are two buttons: 'OK' and 'Cancel'.

5. Enter the SIM ICCID number (up to 20 digits).
6. Click OK. The following screen appears.



A dialog box titled "Source" with a subtitle "IMSI (1-15 digits)". It contains a text input field labeled "Enter IMSI", a checked checkbox labeled "Show Characters", and two buttons at the bottom: "OK" and "Cancel".

**Source**

**IMSI (1-15 digits)**

Enter IMSI

☒ Show Characters

7. Enter the SIM IMSI number (up to 15 digits), then click OK.

The Select Language screen appears.

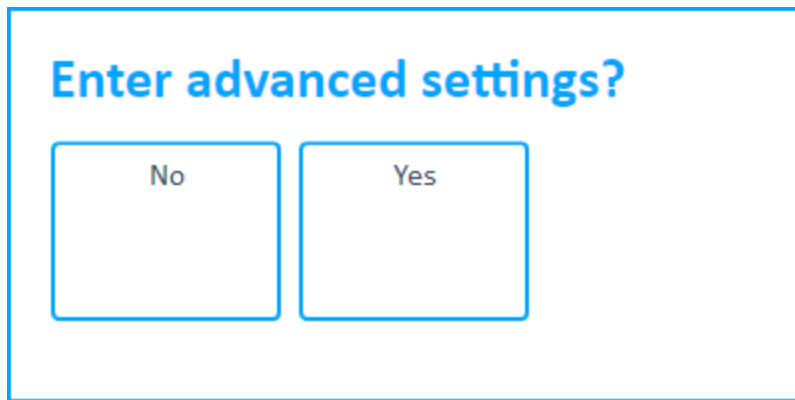


A dialog box titled "LP (optional)" containing a grid of buttons for language selection. The buttons are arranged in three rows: the first row has "None", "German", "English", "Italian", "French", and "Spanish"; the second row has "Dutch", "Swedish", "Danish", "Portuguese", "Finnish", and "Norwegian"; the third row has "Greek", "Turkish", "Hungarian", and "Polish".

**LP (optional)**

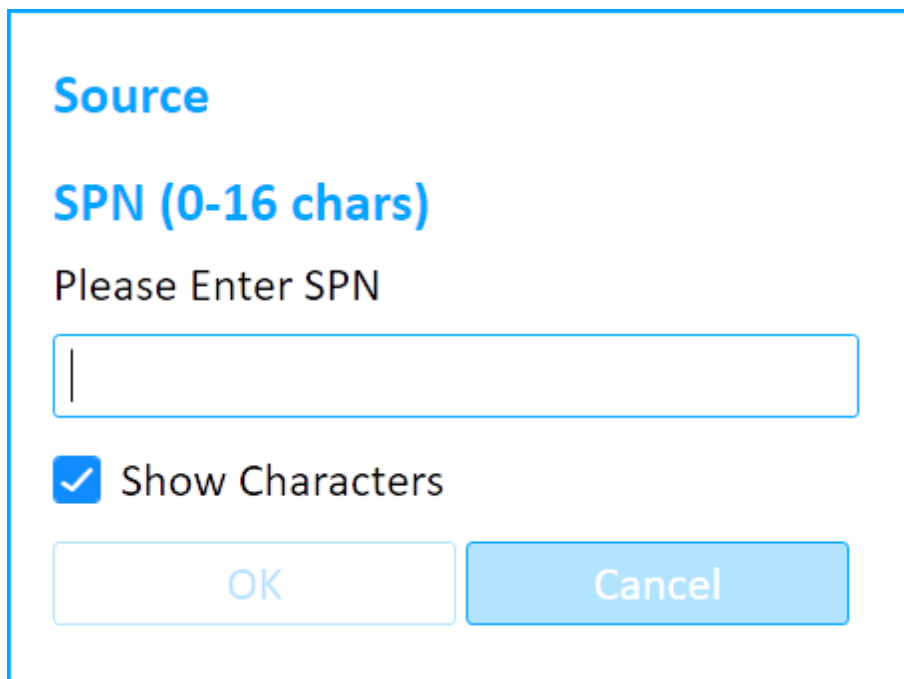
None	German	English	Italian	French	Spanish
Dutch	Swedish	Danish	Portuguese	Finnish	Norwegian
Greek	Turkish	Hungarian	Polish		

8. If required, select either a language or click **None**. The Enter advanced settings screen appears.



A dialog box with a blue border. At the top, the text "Enter advanced settings?" is displayed in blue. Below the text are two buttons: "No" on the left and "Yes" on the right. Both buttons have a blue border and a light gray background.

9. Click **No** or **Yes** to continue.
  - » Click **No** to continue. Proceed to step 15.
  - » Click **Yes** to display the advanced settings. Extraction in Progress > Enter SPN screen appears.



A dialog box with a blue border. At the top, the text "Source" is displayed in blue. Below it, "SPN (0-16 chars)" is displayed in blue. Underneath, the text "Please Enter SPN" is shown in black. A text input field with a blue border is positioned below the text. Below the input field is a checkbox with a blue checkmark and the text "Show Characters". At the bottom of the dialog are two buttons: "OK" on the left and "Cancel" on the right. The "OK" button has a blue border and a light gray background, while the "Cancel" button has a solid blue background.

10. Enter the **SIM SPN** number (up to 16 digits), then click OK. The following screen appears.



The screenshot shows a dialog box titled "Source" in blue. Below the title is the text "GID 1 (0-8 digits)" in blue. Underneath is the instruction "Please Enter GID 1" in black. There is a white text input field with a blue border. Below the input field is a checked checkbox with a blue square icon, followed by the text "Show Characters" in black. At the bottom are two buttons: "OK" and "Cancel", both with blue text and blue borders.

11. Enter the **SIM GID 1** number (up to 8 characters) and click OK. The **Extraction in Progress > Enter GID 2** screen appears.
12. Enter the **SIM GID 2** number (up to 8 characters).
13. Click OK. The Insert Target Card prompt appears.
14. Insert the UFED SIM ID access card into .
15. Click **Continue**.



The Extraction in Progress screen is displayed throughout the data writing process.

At the end of the data writing process, a summary of the SIM cloning process is displayed, detailing the ICCID and IMSI information programmed to the SIM card.

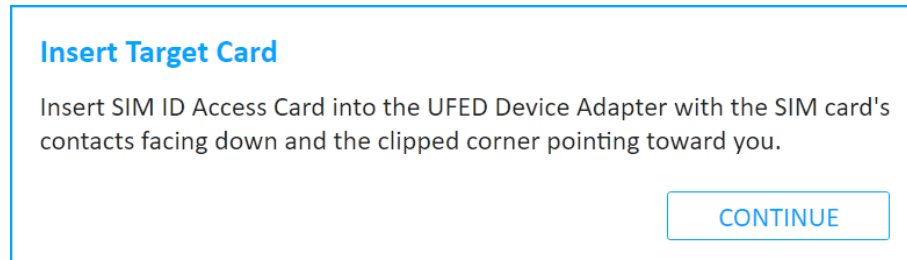
16. To end the process and return to home screen click **Finish**.

### 9.2.3. Creating a GSM test SIM

1. Click **Clone SIM**.

The Waiting for Device screen appears.

2. Insert the SIM card into the SIM card reader slot located in the left of the front panel.
3. Click **Continue**. The Select Source screen appears.
4. Click **Create GSM Test SIM**. The following screen appears.



5. Make sure that the target SIM card is inserted correctly into the SIM card reader slot, then click **Continue**. The Extraction in Progress screen is displayed throughout the data reading process. At the end of the data writing process, a summary of the SIM cloning process is displayed, detailing the ICCID and IMSI information programmed to the SIM card.
6. To end the process and return to the home screen, click **Finish**.

## 10. Drone extractions

UFED enables you to extract flight data and multimedia files from supported drones. You can perform physical extractions, as well capture images of drones. For a complete list of supported drones, refer to the UFED Supported Devices file in [MyCellebrite](#).

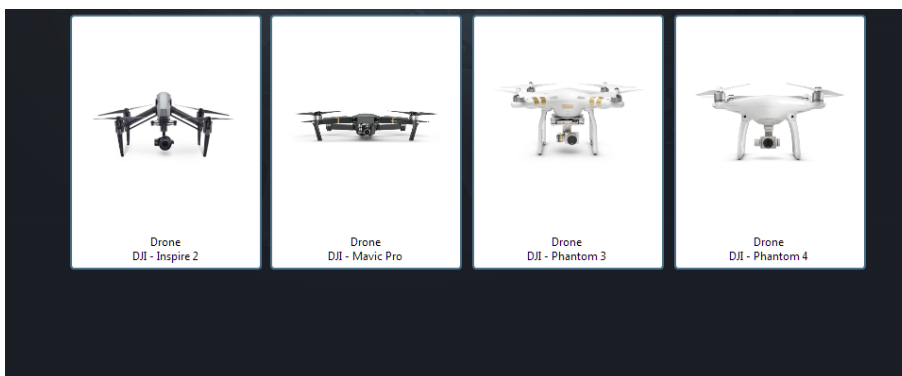
The following example shows how to perform a physical extraction of a drone.

### To perform a drone extraction:

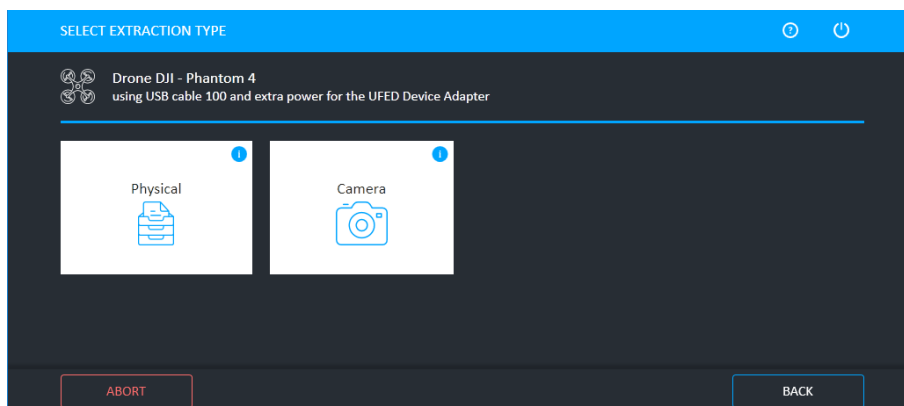
1. Click **Drone**. The following window appears.



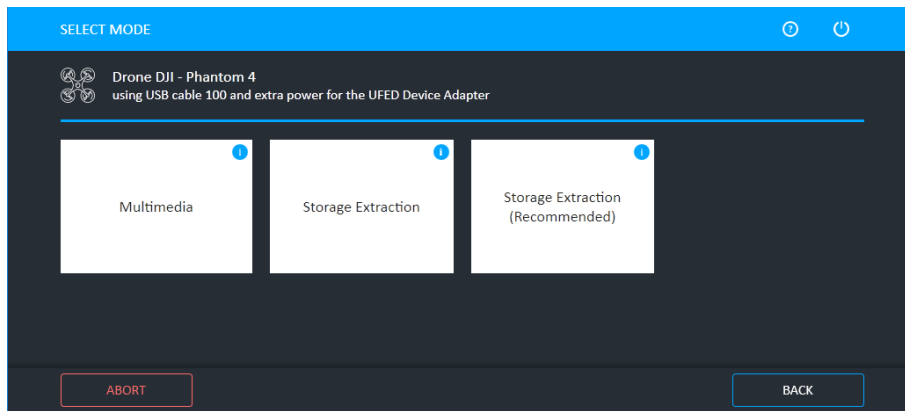
You can also access drones via **Mobile device**, **Mass storage device** or global search.



2. Select the required drone and then click **Next**. The following window appears.



3. Click **Physical**. The following window appears.



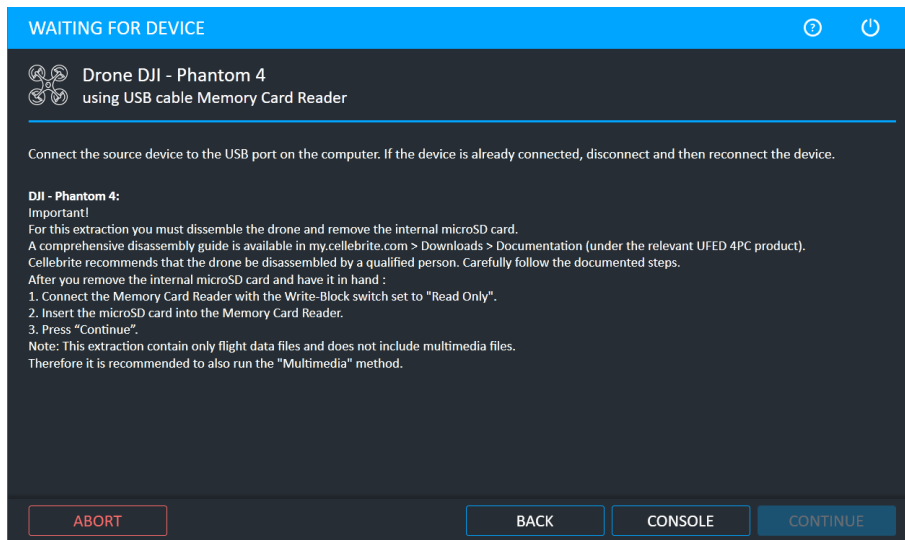
4. Select an option as follows:

- » **Multimedia:** The *external* microSD card stores the multimedia files of the drone i.e., (images and videos) only. To obtain a full data extraction including flight data, it is also recommended to run the "Storage Extraction Recommended" method.
- » **Storage Extraction:** The *internal* microSD card stores the .dat file, which contains the flight data of the drone. The data stored on this card is updated to the time of the extraction. This extraction method is easier than the Storage Extraction (Recommended) mode, but it requires the drone to be turned on which triggers additional log data that is written to the card. This extraction method already includes multimedia files, therefore the Multimedia mode is not required.
- » **Storage Extraction (Recommended):** The *internal* microSD card stores the .dat file, which contains the flight data of the drone. The data stored on this card is updated to the time when the drone was last turned off. This is the recommended extraction method, because the drone stays off and no additional log data is written to the card. However this extraction method is more complicated due to the fact that the microSD card can only be accessed after disassembling the drone. This extraction method does not include multimedia files, therefore it is recommended to also run the Multimedia method. For information on disassembling the drone, refer to [MyCellebrite.com](http://MyCellebrite.com). Cellebrite recommends that the drone be disassembled by a qualified person. Carefully follow the documented steps.



For information on using optional timeframe and party filters, refer to the *Overview Guide*.

The following window appears.



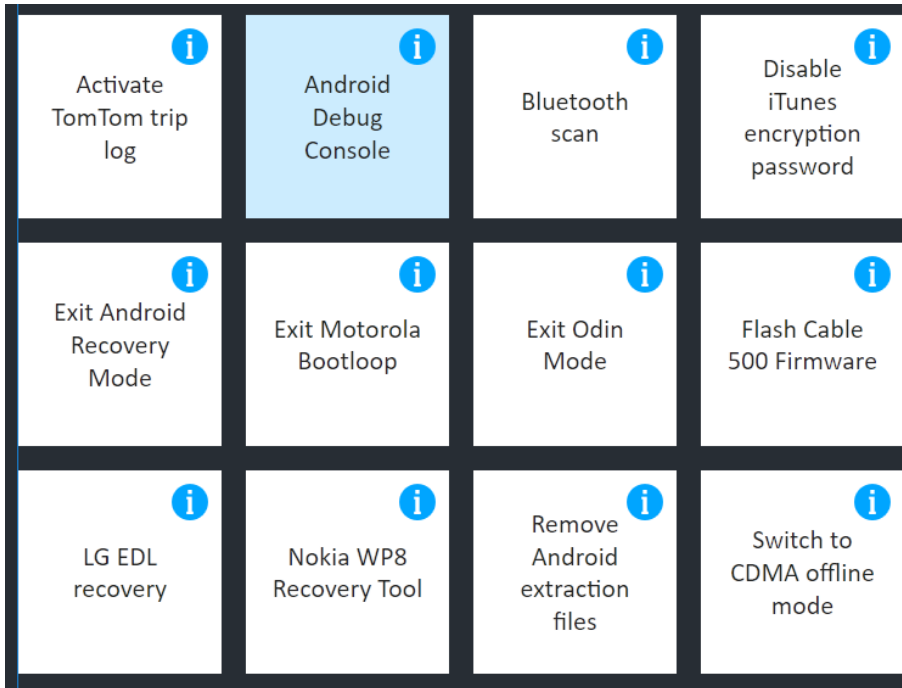
5. Use the specified cable and follow the on-screen instructions.
6. Tap **Continue**.

When the extraction completes, the Extraction completed successfully window appears.

## 11. Device tools

### To access the device tools:

» From the Home screen, click **Device tools**. The following window appears.



The **Device Tools** screen provides access to the following tools:

11.1. Activate TomTom trip log .....	124
11.2. Android Debug Console .....	124
11.3. Bluetooth scan .....	126
11.4. Disable iTunes encryption password .....	126
11.5. Exit Android recovery mode .....	127
11.6. Exit Motorola Bootloop .....	127
11.7. Exit Odin mode .....	127
11.8. Flash Cable 500 Firmware .....	127
11.9. LG EDL recovery .....	128
11.10. Nokia WP8 recovery tool .....	128

11.11. Remove Android extraction files .....	128
11.12. Samsung Exynos Recovery .....	128
11.13. Saved APKs from APK downgrade .....	129
11.14. Switch to CDMA offline mode .....	130
11.15. Uninstall Windows mobile client .....	131

## 11.1. Activate TomTom trip log

This tool enables you to activate or deactivate the trip log logging feature of a connected TomTom device, which is often disabled by the user

### To Activate TomTom trip log:

1. Click **Tools** and then click **Activate TomTom trip log**.

The **Select Mode** prompt appears.

2. Select the desired mode.

A prompt labeled **Attention** appears requesting to connect the device to Cellebrite UFED.

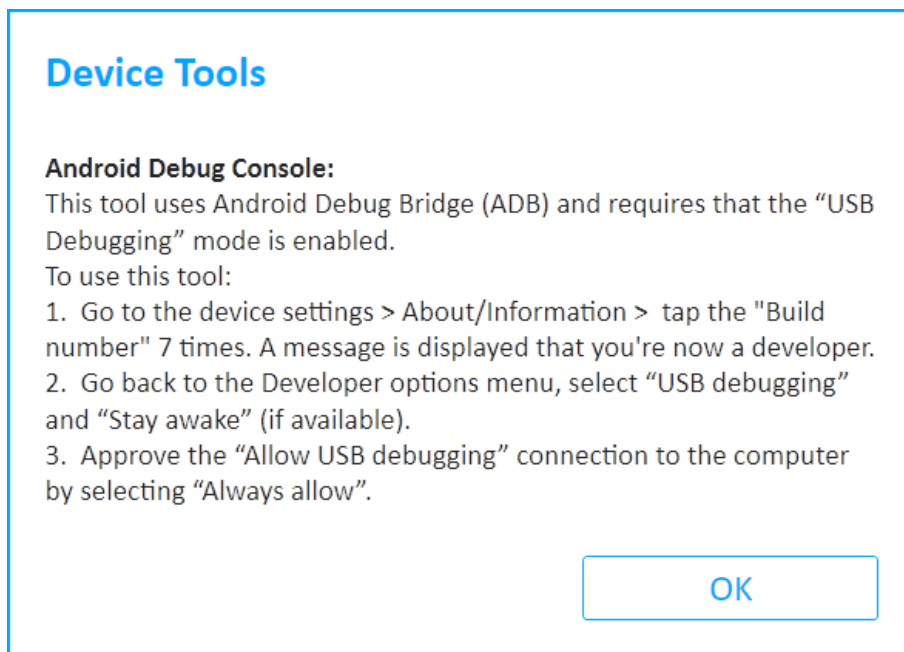
3. Connect the device to Cellebrite UFED.
4. Click **Continue**.

## 11.2. Android Debug Console

This tool retrieves device information using Android Debug Bridge (ADB).

### To use the tool:

1. Click **Tools** and then click **Android Debug Console**.
2. If required, you will be prompted to connect the Cellebrite UFED Device Adapter to a USB port (4PC and non-kiosk platforms only). The following window appears.



3. Follow the on-screen instructions.
4. Tap **OK** to receive the device information. The following window appears.



## Device Info

### USB Descriptors

VID/PID	: 0x1004/0x633E
Manufacturer/Model	: LGE/LGL83BL
Interface 0	: MTP
Interface 1	: ADB Interface

### ADB

Manufacturer/Model	: LGE/LGL83BL
Chipset	: Qualcomm Snapdragon 430

### MSM8937 32 Bit

OS Version	: Android 7.0
Security Patch Version	: 2017-01-01
Encryption State	: encrypted
Rooted	: No
Battery Status (%)	: 90

REFRESH

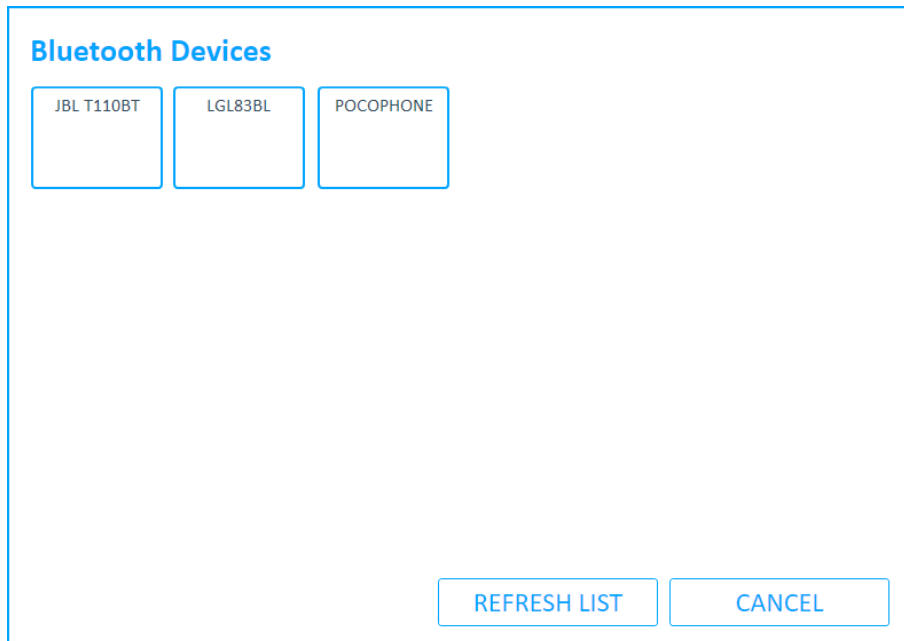
OK

## 11.3. Bluetooth scan

This tool enables you to scan for available Bluetooth devices in your proximity and to pair with them. Make sure that Bluetooth is enabled on the device.

### To perform a Bluetooth scan:

1. Click **tools** and then click **Bluetooth scan**.
2. Connect the Cellebrite UFED Device Adapter (4PC and non-kiosk platforms only).
3. A list of Bluetooth devices in the vicinity appears. Select one or the following options:
  - » Click one of the devices: The Device summary window appears.
  - » Click **Continue**: Device summary window appears
  - » Click **Refresh list**: Device tool in progress window appears and tries to find additional devices.



## 11.4. Disable iTunes encryption password

If you select to enable backup encryption during an iOS File system extraction (Full or Backup modes), and for any reason the extraction was stopped in the middle, the device may remain encrypted. This option resets the encryption on the device.

## 11.5. Exit Android recovery mode

This tool includes two options related to physical extractions using the Forensic Recovery Partition method on Android devices.

- » **Exit recovery mode:** In some cases, due to device failure, or if the mobile device was improperly disconnected from Cellebrite UFED, the mobile device remains in recovery mode. This option enables the device to be taken out of recovery mode.
- » **Exit bootloop:** In some cases, due to device failure, or if the mobile device was improperly disconnected from Cellebrite UFED, the mobile device keeps rebooting instead of entering the normal mode. This option enables the device to be taken out of this bootloop.

## 11.6. Exit Motorola Bootloop

In some cases, due to device failure, or if the Motorola mobile device was improperly disconnected from Cellebrite UFED, the mobile device keeps rebooting instead of entering the normal mode. This option enables the device to be taken out of this bootloop.

## 11.7. Exit Odin mode

To perform physical extractions on some Samsung devices, the device is placed in Odin mode. In some cases, due to device failure, or if the mobile device was improperly disconnected from , the mobile device remains in Odin mode. This option enables the device to be taken out of Odin mode.

## 11.8. Flash Cable 500 Firmware

When using the Smart ADB method, the firmware on Cable No. 500 is changed and will no longer support the Cellebrite UFED User Lock Code Recovery Tool. The Flash Cable 500 Firmware tool flashes the required firmware to the cable to support either the Smart ADB method or the Cellebrite UFED User Lock Code Recovery Tool.



In the Smart ADB method, Cellebrite UFED verifies the cable firmware and flashes it if required. Cellebrite UFED User Lock Code Recovery Tool does not include cable verification.

### To flash the firmware for the Smart ADB extraction method:

1. Click **Tools** and then click **Flash Cable 500 Firmware**.
2. Connect the Cellebrite UFED Device Adapter to a USB port (4PC and non-kiosk platforms only).

3. Connect Cable No. 500 (side A) to the USB port.
4. Tap **Smart ADB Firmware** and wait for the process to finish.

## 11.9. LG EDL recovery

In some cases, due to device failure, or if the mobile device was improperly disconnected from Cellebrite UFED, the LG device remains in emergency download (EDL) mode and appears off. This option enables the device to be taken out of EDL mode.

### To use the tool:

1. Click **Tools** and then click **LG EDL recovery**.
2. If required, you will be prompted to connect the Cellebrite UFED Device Adapter to a USB port (4PC and non-kiosk platforms only).
3. Follow the on-screen instructions.
4. Tap **Continue** and wait for the tool to finish running.

## 11.10. Nokia WP8 recovery tool

To perform physical extraction on some Nokia Windows Phone 8 devices, the device is placed in recovery mode. In some cases, due to device failure, or if the mobile device was improperly disconnected from , the mobile device remains in recovery mode. This option enables the device to be taken out of recovery mode.

## 11.11. Remove Android extraction files

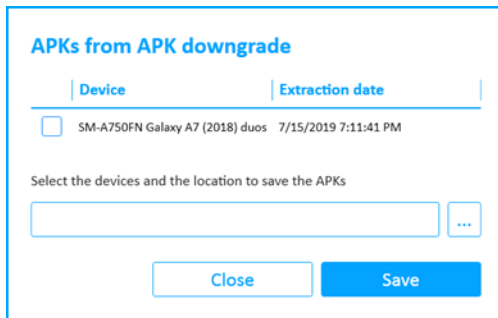
When performing extractions of devices with Android operating systems, a client is installed and some files are written to the mobile device. In some cases (e.g., due to a failure, or if the mobile device was improperly disconnected from ) the client and the files remain on the mobile device. This tool uninstalls the client and removes the files from the device.

## 11.12. Samsung Exynos Recovery

In some cases, due to device failure, or if the mobile device was improperly disconnected from Cellebrite UFED, the device remains off and the Android OS does not start. This option attempts to resolve this issue.

## 11.13. Saved APKs from APK downgrade

This tool saves APKs that could not be reinstalled on the device during an APK downgrade extraction. An example is displayed next.



The screenshot shows a dialog box titled "APKs from APK downgrade". It contains a table with two columns: "Device" and "Extraction date". The first row has a checkbox, the device name "SM-A750FN Galaxy A7 (2018) duos", and the date "7/15/2019 7:11:41 PM". Below the table is a label "Select the devices and the location to save the APKs", followed by a text input field and a button with three dots "...". At the bottom are two buttons: "Close" and "Save".

	Device	Extraction date
<input type="checkbox"/>	SM-A750FN Galaxy A7 (2018) duos	7/15/2019 7:11:41 PM

Select the devices and the location to save the APKs

...

### To save the APK:

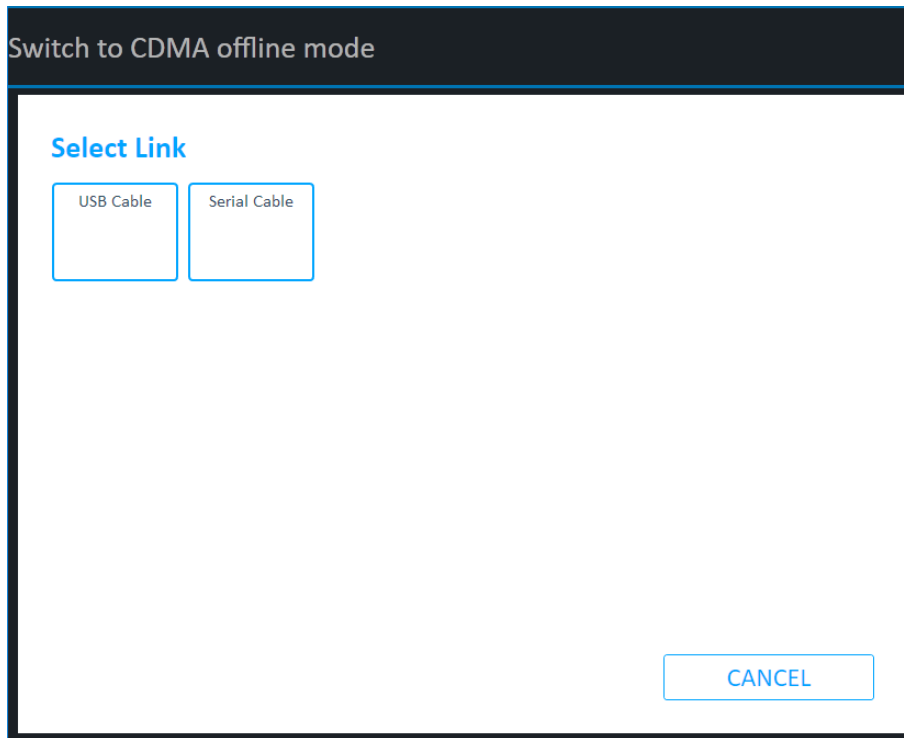
1. Select the device.
2. Select the location where the APK should be saved.
3. Click **Save**.

## 11.14. Switch to CDMA offline mode

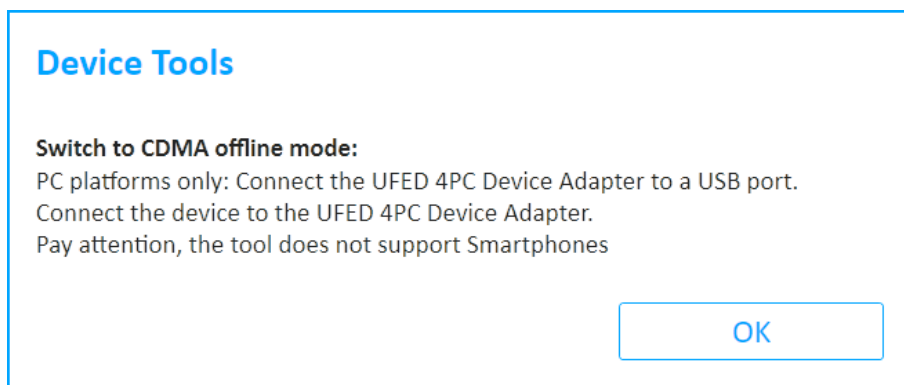
This tool enables you to switch radio on CDMA devices to offline mode.

**To switch to CDMA offline mode:**

1. Click **tools** and then click **Switch to CDMA offline mode**.
2. Connect the Cellebrite UFED Device Adapter (4PC and non-kiosk platforms only). The Select Link prompt appears.



3. Select the link type (**USB Cable** or **Serial Cable**). The Device Tool in Progress window appears.



4. Tap OK.

Upon completion, the Device Tool Summary appears.

## 11.15. Uninstall Windows mobile client

To perform logical extractions on devices with Windows Phone operating systems, a client is installed on the device. In some cases, due to a device failure, or if the mobile device was improperly disconnected from , the client remains installed on the mobile device. This option enables the client to be manually uninstalled.

## 12. Glossary

---

### C

---

#### CAS

Cellebrite Advanced Services (CAS) offers customers the ability to recover valuable evidence from heavily damaged, locked or encrypted devices.

#### Cellebrite UFED 4PC

Enables users to deploy extraction capabilities on Windows based tablets, laptops, and desktop computer systems. It performs physical, logical, file system and password extractions on a wide range of devices.

#### Cellebrite UFED Touch

Enables the simplified extraction of mobile device data. Depending on the license purchased, it performs physical, logical, file system and password extractions on a wide range of devices.

---

### P

---

#### Physical/Logical Analyzer

An analysis and reporting tool for logical, file system and physical extractions. This software solution provides users with the capability to extract data, perform advanced analysis, decoding and reporting and presenting the results in a clear and concise manner.

---

### U

---

#### UFED

Universal Forensic Extraction Device



## 13. Index

### A

Accessories 10

ADB, definition 60

Android backup 41, 44-45, 50

Android backup APK downgrade 45, 50

APK downgrade 45, 50

### B

Bluetooth scan 126

Bluetooth, logical extraction 24

Boot Loader, definition 60

### C

Capture 9, 95, 101-102

Capture images 9, 95-96, 119

Capture images and screenshots 10, 95

Cellebrite YouTube channel 14

Clone SIM 9, 107, 111-112, 114, 118

Cloning an existing SIM card ID 111

### D

Device tools 122

Drone, extractions 119

### E

Entering SIM data manually 114

Exit Motorola bootloop 127

Extracted passwords folder 32

Extracted SIM data folder 110

Extraction in progress 30, 40, 61, 64, 84, 90, 113, 116, 118

Extractions, (Refer to Performing extractions in MyCellebrite) 9, 16, 32

### F

File system extraction 9, 38, 107, 126

File system extraction folder 40

Files, logical extraction type 22

Flashing 82

Forensic recovery partition 87

FW flashing 82

### G

GSM test SIM 118

### H

Help 15

Home screen 32, 66, 73, 122

### I

iOS extraction 17

iTunes backup encryption 20

### J

JTAG 45

### L

Legal notices 2

Logical extraction 7, 9-10, 14-17, 20-21, 24, 107

## N

Nokia WP8 recovery tool 128

## O

Odin mode 127

Overview 7, 12, 17, 21, 38, 41, 46, 50, 56, 60, 63, 66, 82, 85, 88, 91, 120

## P

Password extraction 9, 29

Performing a file system extraction 38

Performing a physical extraction 60

Performing extractions 1

Performing SIM data extraction 107

Physical extraction 9, 56, 59-60, 62-63, 65, 82, 85, 87, 128

## Q

Qualcomm chipsets 85

## R

Re-enable User Lock option 33

Rooted Android devices, physical extraction 63

## S

Samsung Exynos Recovery 128

Screenshots 10, 95, 100, 103

Select content types 14

Select extraction location 82

Settings 41, 66

SIM data extraction 107, 110

SIM extraction 9

Smart ADB method, tool 127

Specifications 2, 12

Specify a network location 53, 120

Supported devices 14

Switch to CDMA offline mode 130

System requirements 8

## U

UFED Device Adapter 11, 13, 124, 126-128, 130

UFED User Lock Code Recovery Tool 127

Unallocated space 9

Using cables and tips 13

## W

Working with TomTom 124